CM-400-260-01: Vol. 1 of 1

Revision 2.0: 8 July 1997

SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

FOR THE

NETWORK MANAGEMENT (NM) FUNCTIONAL AREA

OF THE

DEFENSE INFORMATION INFRASTRUCTURE (DII) COMMON OPERATING ENVIRONMENT (COE)

This document is **UNCLASSIFIED** in its entirety

Prepared for and by:

Defense Information System Agency (DISA)
Joint Interoperability and Engineering Organization (JIEO)
Center for Computer Systems Engineering (CFCSE)
DII COE Engineering Office (JEXF-OSF)
Operational Support Facility
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Intentionally Left Blank

Signature Sheet

The Software Requirements Specification (SRS) for the Network Management (NM) functional area of the Defense Information Infrastructure Common Operating Environment (DII COE), Revision 2.0, 8 July 1997:

SUBMITTED BY:

_____

Gregory A. Csehoski, Major, USAF
Chairperson,
DII COE Network Management Technical Working Group (NETTWG)
Joint Interoperability and Engineering Organization
Defense Information Systems Agency

APPROVED BY:

_____

Dawn A. Hartley,
DII COE Chief Engineer,
Center for Computer Systems Engineering
Joint Interoperability and Engineering Organization
Defense Information Systems Agency

Table of Contents

NOTE: This document is maintained by the Chairperson, DII COE Network Management Technical Working Group. Comments concerning this document should be submitted electronically to the Chairperson, Major Gregory A. Csehoski, at csehoskg@ncr.disa.mil or via the mailing address on the front cover of the document.

List of Figures

List of Tables

1. Scope.

1.1 Identification.

This Software Requirements Specification (SRS) describes the requirements for the Network Management (NM) functional area of the Defense Information Infrastructure (DII) Common Operating Environment (COE). The NM Services functional area falls under the overall Management Services functional area. This SRS is limited to network management functional concerns and does not address the entire Management Services arena of the DII COE.

The SRS is independent of a particular DII COE version. Instead, this document contains the total objective set of DII COE network management requirements that DISA, as the Executive Agent (EA) of the DII COE, strives to fulfill. This document only applies to those network management applications that are considered an integral part of the DII COE and fall under the direct control and supervision of the DII COE Engineering Office (DISA/JEXF-OSF). There may be cases where network management applications are in use by DII COE-compliant systems but they are not considered part of the DII COE because they are not under the DII COE Engineering Office's direct control and supervision. These unique sets of network management applications are considered mission applications for use exclusively within their community of interest. They fall outside the scope of this SRS.

1.2 System Overview.

1.2.1 Architecture Versus System.

To view the COE as a command, control, communications, computers, and intelligence (C4I) system is incorrect because it misses the fundamental point that the COE is *not* a system; it is a *foundation* for building an open system. This viewpoint also makes fielding and update schedules confusing because it fails to account for the impact of the evolutionary development strategy. To view the DII COE as the Global Command and Control System (GCCS) or just as an architecture gives the mistaken impression that its principles are limited to the GCCS program. GCCS is simply the first system built using the DII COE while the Global Combat Support System (GCSS) is in progress. Many other Service and Agency (S/A) programs are now in the process of migrating to the DII COE.

Building a target system, such as Defense Information Systems Network (DISN) Management Centers, GCCS, or GCSS, is largely a matter of combining COE components with mission specific software. The COE infrastructure manages the flow of data through the system, both internally and externally. Mission specific software is mostly concerned with requesting data from the COE and then presenting it in a form that is most meaningful to the operator (e.g., as a pie chart, in tabular form, as a graph). The COE provides the necessary primitives for such data manipulation, and has the necessary information about where the requested data is stored,

whether locally or remotely across the local area network (LAN) or wide area network (WAN). This frees the system designer to concentrate on meaningful data presentation and not on the mechanics of data manipulation, network communications, database storage, etc.

It must be kept in mind, however, that there is only one COE. Each system uses the same set of APIs to access common COE components, the same approach to integration, and the same set of tools for enforcing COE principles. Systems are built on top of the COE and use precisely the same COE software components, not just the same algorithms, for common functions (e.g., communications interfaces, data flow management). This approach to software reuse significantly reduces interoperability problems because if the same software is used, two dissimilar mission systems will interpret or implement these common APIs and get the same results.

The DII COE concept is best described as an architecture that is fully compliant with the *DOD Technical Architecture for Information Management (TAFIM), Volume 3*; an **approach** for building interoperable systems; a **reference implementation** containing a collection of **reusable software** components; a **software infrastructure** for supporting mission-area applications; and a set of **guidelines, standards, and specifications**. The guidelines, standards, and specifications describe how to reuse existing software and how to properly build new software so that integration is seamless and, to a large extent, automated. The DII COE will evolve as necessary to become compliant with emerging specifications, such as the *Joint Technical Architecture (JTA)* and the TAFIM. The JTA stipulates DII compliance as part of its requirements and replaces the standards guidance in the TAFIM as per an OSD directive dated 30 August 1996.

The objective of the Network Management Technical Working Group (NETTWG) is to provide the end-user community with DII COE-compliant network management applications. The applications are broken into two broad categories. The first would be those applications that are run out of a management center such as a Simple Network Management Protocol (SNMP) manager. This category of applications would be installed on DII COE-compliant workstations or servers which function primarily as management workstations. The other category of applications would be those components that run on end-user workstations, application servers, data servers, and so forth which remotely gather management information. This category of applications can be considered monitoring or reporting agents to the higher level management center. Combining these two categories of network management applications will give the designer of a DII COE-compliant system the tools necessary to effectively perform network management of their system.

The goal of the NETTWG is to create a library of segmented applications that can be used by any chief engineer in the design and creation of their system. The library will consist mostly of commercial-of-the-shelf (COTS) management software. However, some management applications will be government-of-the-shelf (GOTS) because they will provide specialized management functionality unique to the warfighter's domain. It is envisioned that all COTS network management applications will fall under the control and supervision of the DII COE Engineering Office and be considered integral components of the DII COE. It is unlikely that any

COTS network management application would be considered a unique mission application since this would severely limit its software reusability across DOD without incurring significant duplication of costs.

The following sections help to further describe the DII COE architecture and the various systems that will be based on the DII COE. DISA has been mandated by the Office of the Secretary of Defense (OSD) as the global provider of networks for the DOD warfighter. The DISN and its subcomponents, is a major component of the DII and is operated and maintained by DISA. However, the DII also includes the Defense Switch Network (DSN) for voice communications, the Defense Satellite Communications System (DSCS) for space-based communications, and a multitude of other networks of various technologies. These globally-based networks are the focal points for combining Service and Agency (S/A) networks, specialized metropolitan area networks (MANs), base, post, campus local area networks (LANs), and others together to form the heterogeneous DOD communications infrastructure. Some of the communications systems are briefly described below to help one understand the complexity and source of requirements for network management applications operating on the DII COE.

1.2.2 Defense Information Infrastructure (DII) Common Operating Environment (COE) Architecture.

For detailed information on the DII COE please consult the *Defense Information Infrastructure (DII), Common Operating Environment (COE), Integration and Runtime Specification (I&RTS), Version 2.0, dated October 23, 1995* and the *Defense Information Infrastructure (DII), Common Operating Environment (COE), Integration and Runtime Specification (I&RTS), Version 3.0, dated January 1997.* These documents are instrumental in providing a common starting point for learning and understanding the DII COE. The documents also provide a detailed breakdown of the functional areas within the DII COE. As stated earlier, the DII COE provides the foundation on which systems are built. Once one grasps the fundamental principles of the DII COE it is easy to see how the various support components of the different communications systems can be built upon DII COE-compliant workstations and servers.

1.2.3 Defense Information Infrastructure Control Concept (DIICC).

The goal of the DII program is to provide a seamless end-to-end integration of DOD's information resources. A unified view of all infrastructure components is to be provided by the DIICC. DIICC will provide a fused, real-time representation of the three-dimensional battle space. The wide range of DOD operations clearly demonstrates the need for a DIICC that is flexible enough to ensure and maintain mission integrity independent of geographical location or environment.

The DIICC takes a more open-systems view of information infrastructures. Figure 1 is a view of the systems and network management data flow between DII elements. Note that this view is

non-hierarchical in nature. On the outer ring are the Base-level Network Control Centers (BNCCs), the DSCS, the System Management Centers (SMCs), the Local Control Centers (LCCs), etc. These various centers are the management information providers. The Management Information Bases (MIBs) and alerts from management software move inward to the DISN Regional Control Centers (RCCs) and finally, after aggregation, to the Global Operations and Security Center (GOSC). Both the status information and aggregate information can be transmitted outward from the RCCs.

The DII/DISN GOSC and RCCs depicted in the figure are the responsibility of DISA DISN organization. Unfortunately, responsibility for the outer ring is not so clearly established. Some entities are under the responsibility of DISA while others are the responsibility of various communities of interest or the S/As. Some of the management entities are based on a base, post, campus location and others are unique to a building or facility complex. Some programs like GCCS have multiple layers of management centers. A two-tiered concept is used for managing the GCCS with a primary LCC taking care of the Joint Staff oversight mission out of the Pentagon and then the individual secondary LCCs at the base, post, and campus locations performing the day-to-day operations. A major concern of any system engineer building a network control center will be to ensure that the direction taken by the particular program or mission is in concert with the long term goals of the DIICC.

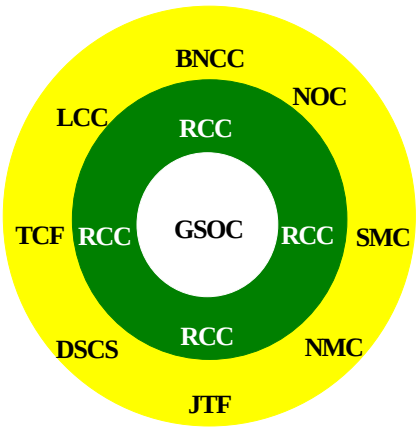

Figure 1: DIICC Management Information Data Flow.

The DIICC system and network management strategy uses the OMNIPoint systems and network management model shown in Figure 2. The five management services defined by the International Standards Organization's (ISO) Common Management Information Protocol (CMIP) are shown in the middle of Figure 2. Feeding these services are Service Delivery Points from commercial providers, Communications Elements (CEs), Information Processing Elements, Value-Added Services Elements, and the User Equipment Elements.

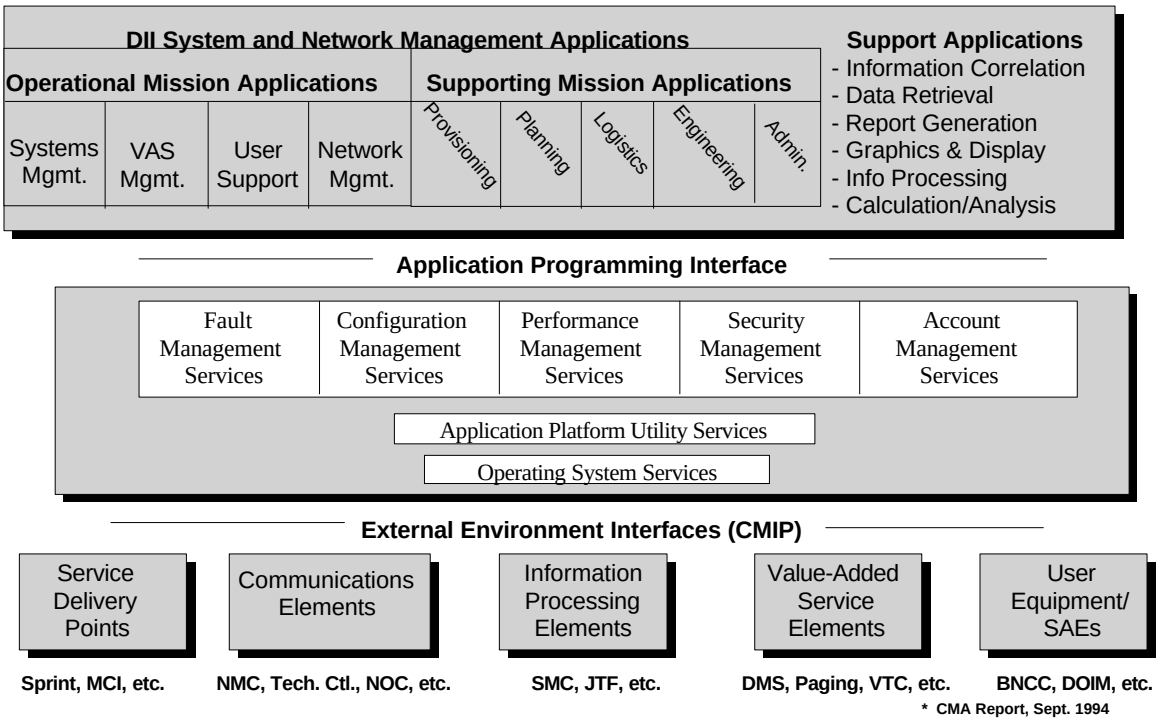

Figure 2: DIICC OMNIPoint Perspective.

The essential DIICC value added is the correlation analysis function. The DIICC can make sense of seemingly unrelated inputs emanating from a wide variety of dispersed locations to isolate and determine the origin of a fault anywhere within the system. The DIICC can see all anomalies concurrently and proactively correlate the errors during the fault detection process. It can then broadcast to the appropriate parties the status of the problem and the steps being taken to fix it.

OMNIPoint was organized by the Network Management Forum (NMF). Its purpose is to analyze current standards and establish a progression of steps to specify the most robust systems and networks management possible. The focus for OMNIPoint is basic interoperability between systems and products for fault management and configuration management. The OMNIPoint partners have selected standards and technologies that can be used in multiple combinations to support different environmental, budgetary, and functional requirements. Element managers, for example, use either the Simple Network Management Protocol (SNMP) or the Common Management Information Protocol (CMIP); both are specified. The OMNIPoint requirements reference technology from many different sources, such as Open Software Foundation (OSF), Distributed Computing Environment (DCE), the Object Management Group (OMG), Common Object Request Broker Architecture (CORBA), and the X/Open Management Protocol (XMP)

communications interface. OMNIPoint defines several phases with each phase making progress toward a totally integrated and interoperable management structure.
Current information on the DII, the DIICC, and the OMNIPoint status can be obtained by contacting the DISA/D3 office at commercial (703)-735-6680 or DSN 653-6680.

1.2.4 Defense Information Systems Network (DISN).

The DISN is a collection of voice and data networks composed of multiplexers, cryptographic devices, routers, and other devices combined to create a worldwide information transfer infrastructure. The DISN evolved from two directions. The first was the need to replace the Defense Data Network (DDN). The second was a study conducted in September 1991 by the Office of the Assistant Secretary of Defense for C3I (OASD/C3I). The study directed DISA to implement the recommendations of an OASD/C3I chaired Task Force which had investigated alternatives for the evolving DOD communications. The five major goals were:

- Establish a foundation for providing subscriber-to-subscriber transport service infrastructure
- Consolidate independent DOD networks into a transport service for providing interoperability, resource sharing and consolidation
- Provide faster provisioning and more responsive customer support
- Capitalize on COTS products and international standards to create an open, non-proprietary architecture
- Reduce DOD telecommunications costs

One of the data portions of the DISN consists of router-based layers, each of a different classification level. The unclassified router layer is the Unclassified Internet Protocol Router Network (NIPRNET) which replaced MILNET. The secret router layer is the Secret Internet Protocol Router Network (SIPRNET) which replaced DSNET1. No top secret router network was built to replace DSNET2. No DOD organization currently requires a standalone, robust, physically separate, top secret WAN. However, several communities of interest do require a global top secret WAN-like capability. This is provided by tunneling through one of the other DISN networks (NIPRNET or SIPRNET) using end-to-end encryption (E^3) devices for encrypting the datagrams. These encrypted top secret datagrams can then use either the NIPRNET or the SIPRNET for data transport. The final layer is the top secret/sensitive compartmented information router network called the Joint Worldwide Intelligence Communications System (JWICS) that replaced DSNET3. This network is not under DISA control and is not considered a component of the DISN. It is owned by the Defense Intelligence Agency (DIA).

Figure 3 shows the router layers of one segment of the data portion of the DISN's overall architecture. Each layer is shown as a separate entity. The E^3 devices mentioned above are certified multi-level security (MLS) cryptographic devices that will allow for data of one classification level to ride on a different DISN router layer for data transport. Two predominant

types of E^3 devices in use are the BLACKER system or the Motorola Network Encryption System (NES). The BLACKER system is used by a group of secret-level Air Force (AF) subscribers who use the unclassified router layer (NIPRNET) for their data transport. The NES is used by the Top-Secret Support System (TS3) portion of the GCCS. The TS3 sites operate at the top secret layer but use SIPRNET for data transport. DOD communities must be aware of the existence of these E^3 capabilities. They play an important role in how various communities of interest users are all interconnected in the virtual network. Their existence in the system and technical operating parameters must be understood so proper system and network management can be performed.

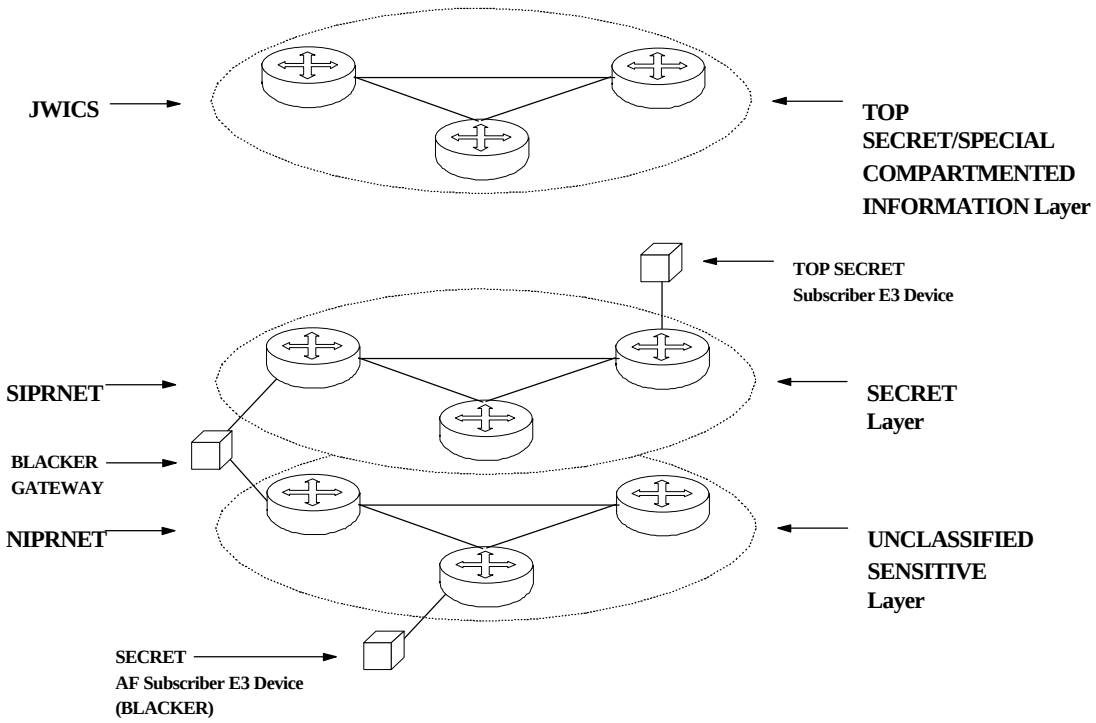

Figure 3: DISN Internet Protocol Router Layer Architecture.

1.2.4.1 DISN Network Management Hierarchy Model.

The DISN uses a three-layer model to define the different areas of network management responsibility. Figure 4 graphically depicts the model while concentrating on a SIPRNET viewpoint. The top level DII control center is referred to as the Global Operations and Security Center (GOSC) which is operated by the DISA C4I Network Systems Management Division (D31). The GOSC provides management oversight for the networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, the NIPRNET, the defense satellite networks, the Network Equipment Technologies, Inc. Integrated Digital Network Exchange (IDNX) multiplexer networks, the Defense Switch Network (voice), AUTODIN, and others to name a few. The second layer consists of the Regional Control Centers (RCCs). The RCCs are responsible for the day-to-day operations of the networks under their immediate control. They are geographically oriented with several centers dispersed across the

United States; a center located at the DISA European facilities to cover Europe, and another located at the DISA Pacific facilities to cover the Pacific assets. The RCCs are responsible for the DISA assets within their areas and operate as peers to each other. The RCCs responsible for various portions of the NIPRNET and SIPRNET are also responsible for the health of the DISN routers installed on those networks. The Scott AFB RCC is responsible for the IDNX multiplexer network.

The RCCs and the GOSC are responsible for DISA assets only. They do not control any assets owned by the individual S/As connected to the networks or WANs. The customer premise routers are included in the list of equipment that the GOSC and the RCCs do not manage unless this fee-for-service capability has been purchased. It is the responsibility of the individual communities of interest, i.e., the individual sites or support organizations, to manage their own assets. This is where the third layer of the hierarchy model comes in to play. These management centers, or DII control centers, are referred to as Local Control Centers (LCCs) and they belong to the individual subscriber communities.

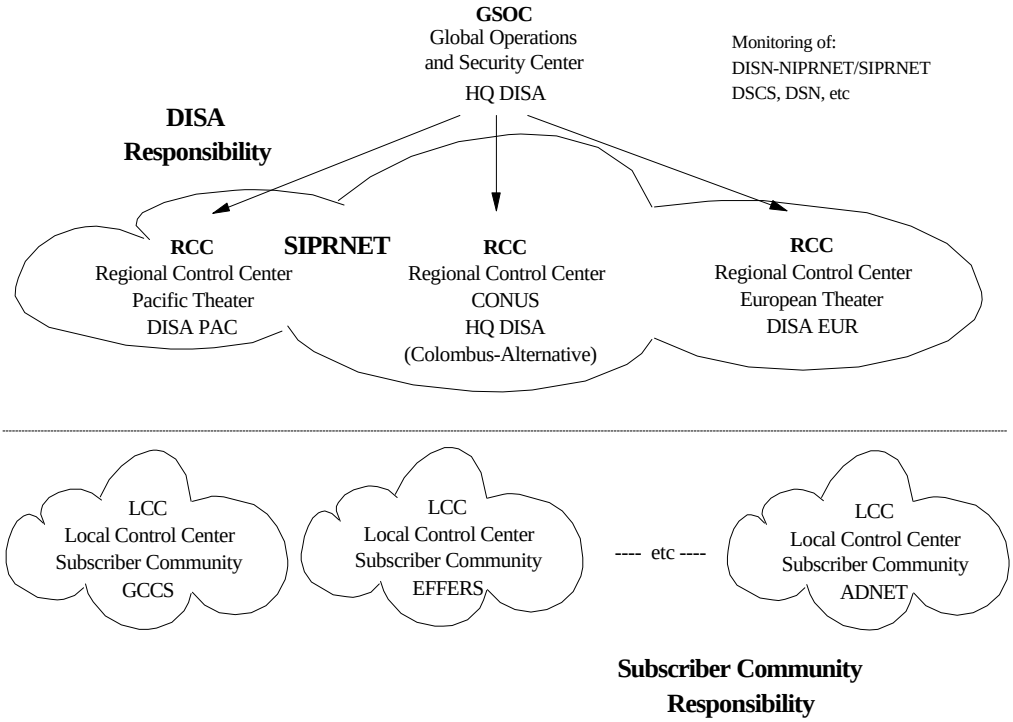

Figure 4: DISN Network Management Hierarchy Model.

1.2.4.2 Secret Internet Protocol Router Network (SIPRNET).

The SIPRNET is the worldwide router-based network that replaced the older X.25-based packet switched network DSNET1 of the DDN. The initial SIPRNET backbone router network went online 3 March 1994. Subscribers started coming online shortly thereafter. The SIPRNET WAN consists of more than 45 operational backbone routers interconnected by high-speed serial links to serve the long-haul data transport needs of secret-level DOD subscribers. SIPRNET supports the DOD standard Transmission Control Protocol/Internet Protocol (TCP/IP) protocol service. Provisions are made in the described SIPRNET architecture to support the Government Open Systems Interconnection Profile (GOSIP) router protocol service at a future date. Currently, no subscribers require immediate GOSIP protocol service on the SIPRNET. Subscribers within the DOD and other Government Agencies are able to use the SIPRNET for passing datagrams at the Secret-US Controlled classification level. The Secret-Not Releasable to Foreign Nationals (SECRET-NOFORN) classification level was removed from the SIPRNET in late CY95. Additionally, the NOFORN caveat has been changed to U.S. ONLY in security classification guidance documentation. There will be instances where connections to agencies of foreign governments or to other networks of a different classification level exist. These connections will be via an accredited security guard device that will prevent unauthorized or accidental disclosure of NOFORN or other caveated classified information from the SIPRNET.

The SIPRNET is managed by the DII/DISN RCCs which provide day-to-day operational management. The RCCs use a variety of network management products to evaluate any router on the SIPRNET. Data is collected on various traffic patterns within the SIPRNET. Data collection includes total router traffic sent and received. The results of the various data collecting efforts are kept on file for long term management of the router-to-router traffic.

For current information on the SIPRNET concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8290 or DSN 653-8290. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

1.2.4.3 Unclassified Internet Protocol Router Network (NIPRNET).

The NIPRNET is the worldwide router-based network that replaced the older X.25-based packet switched network MILNET of the DDN. The NIPRNET WAN consists of more than 120 operational backbone routers interconnected by high-speed serial links to serve the long-haul data transport needs of unclassified-level DOD subscribers. Like SIPRNET, the NIPRNET supports the DOD standard TCP/IP protocol service.

The NIPRNET is also managed by the DII/DISN RCCs which provide day-to-day operational management. Again, the RCCs use a variety of network management products to evaluate any router on the NIPRNET and data is collected on the various traffic patterns on the network.

For current information on the NIPRNET concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8484 or DSN 653-8484. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

1.2.4.4 Dial-in Capabilities via DISN Communications Servers.

Communications Servers (CSs) were added to the NIPRNET and SIPRNET WANs during FY95 for the general DOD community. These CSs are managed by the DII/DISN RCCs responsible for that area of the WAN. The CSs give remote subscribers the capability to access the NIPRNET or SIPRNET WANs via dial-in. This capability is especially valuable for those subscribers who do not have the need for a dedicated connection, for those subscribers who are continually traveling on temporary duty (TDY), or for deployed tactical subscribers who have access to a telephone system.

The NIPRNET uses standard Hayes-compatible modems for the audio connectivity. The SIPRNET uses AT&T STU-III Model 1910 to provide dedicated wireline encryption of the dial-in link. The CSs deployed on the WANs are Cisco 2511-CSs which are capable of 115 kbps throughput on the dial-in ports. However, some dial-in links were initially limited to a maximum throughput of 19.2 kbps to accommodate all makes and models of modems and compatible secure telephone units (STUs) in use by the DOD. The CSs are capable of supporting Point-to-Point Protocol (PPP), Compressed PPP (CPPP), Serial Line Interface Protocol (SLIP), Compressed SLIP (CSLIP), along with Telnet, Kermit, and other functions.

Both strategic and tactical DOD communities-of-interest can take advantage of the DISN CSs available on the NIPRNET and SIPRNET WANs provided they are registered users. Again, the day-to-day operational management of the CSs will be by the DII/DISN RCCs. It is important to note that like the DISN router service, there is a fee for becoming a registered user of the DISN CSs. The published tariff is $10 per month per individual user with a one-time $45 registration fee. For current information on the DISN CSs concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8355 or DSN 653-8355. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

1.2.4.5 Integrated Tactical Strategic Data Networking (ITSDN).

The ITSDN Quick Fix Program installed gateway routers to support deployed Joint Task Force (JTF) contingencies, exercises, and training missions with requirements to interface with the DISN Internet Protocol Routers (IPRs). The goal of the DOD, in general, and the ITSDN gateway routers, specifically, is to be able to support two contingency operations in different parts of the world simultaneously. The program installed 2 routers at each of 10 globally located strategic Ground Mobile Force (GMF) entry points. The 20 gateway routers are divided into 2 sets of 10 routers each based on the classification of data they process. The first set of routers connects tactical subscribers to strategic networks via the SIPRNET. The other set of routers

connects tactical subscribers to strategic networks via the NIPRNET. Each entry point received two routers, one for unclassified traffic and the other secret for secret traffic. The ITSDN routers support the standard TCP/IP protocol suite for serial or Ethernet connections. SIPRNET and NIPRNET are two of the IP router layers previously defined in the DISN router architecture model.

The ITSDN entry point suite of equipment consists of an unclassified router, a secret router, cryptographic equipment, and other ancillary devices. The 10 suites of equipment allow tactical forces access to strategic systems via the DSCS through a Defense Communications System Entry Point (DCS-EP). These EPs provide worldwide access for JTFs. Some documents being produced may refer to the DCS-EPs as Defense Information System Network Entry Points (DISN-EPs). Both are valid. Additionally, the DCS-EPs are undergoing upgrades. Once an upgrade is complete, the location is referred to as a DISN Standardized Tactical Entry Point (STEP).

The tactical subscribers' connections are serial connections provided by satellite communications equipment at the DCS-EP sites. The ITSDN gateway routers support the standard TCP/IP protocol suite for serial connections to the gateway routers.

Deployed forces may rely on the ITSDN capabilities to reach either the NIPRNET or the SIPRNET WANs. The DII/DISN RCCs provide day-to-day operational management of the ITSDN routers.

For current information on ITSDN concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8355 or DSN 653-8355. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

1.2.4.6 Joint Defense Information Infrastructure Control Center - Deployed (JDIICC-D).

To be added later.

1.2.4.7 DISN Management Demarcation Point.

A major concern of system and network management responsibilities is determining where the demarcation points exist within a particular system. This can be discussed in terms of physical locations, management control, and/or the ownership of the workstation, servers, communications equipment, and other hardware devices. This vast array of demarcation points may also exist along political, technical, or programmatic lines. The diversity of demarcation points will require network management applications to have the ability to support a widely divergent class of network management domain.

One primary demarcation point that exists for the majority of DOD systems will be the one between the subscriber community's communications equipment and the DISA DISN equipment. As alluded too before, the DISA GCC and RCCs do not manage assets belonging to subscriber communities. While this definition provides a starting point, it does not provide the exact physical location of change over. The demarcation point for SIPRNET serial access circuits has been defined more completely by stating the RED (unencrypted, clear-text classified information) side of the cryptographic equipment installed in the subscriber's location is where DISA GOSC and RCCs responsibilities end and the subscriber's responsibility begins. The demarcation point for NIPRNET serial access circuits is defined more completely by stating the data terminal equipment (DTE) side of the modem equipment installed in the subscriber's location is where DISA GOSC and RCCs responsibilities end and the subscriber's responsibility begins. The demarcation points exist at these locations because the DISN RCCs are responsible for the health and maintenance of the serial access circuits. Typically, DISN cryptographic, modem, and other ancillary devices are located in the subscriber's area. Arrangements are made during the provisioning process on how the DISN-owned equipment will be maintained. In the case of Ethernet connections, the subscriber's responsibility is from the servicing Ethernet port on the DISN backbone router to their assets. The DISN RCCs do not manage the site's LAN. It is possible that a site with an Ethernet connection to the DISN can still have a premise router in the communications path. To reenforce these definitions, Figures 5 and 6 are included to show the demarcation points. The two drawings help show how the demarcation point differs for the two types of connections. Again, the primary difference is the DISN RCCs are responsible for restoration of the serial access circuits. The vast majority of DISN access connections are serial in nature and not Ethernet.

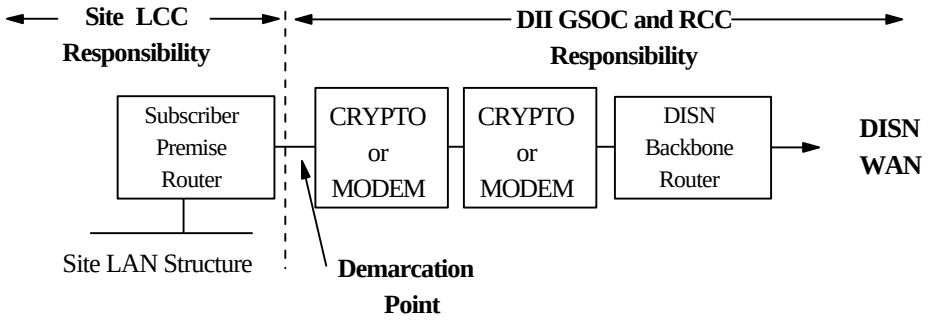

Figure 5: Demarcation Point of Responsibility for Serial Access Circuits to DISN Networks.

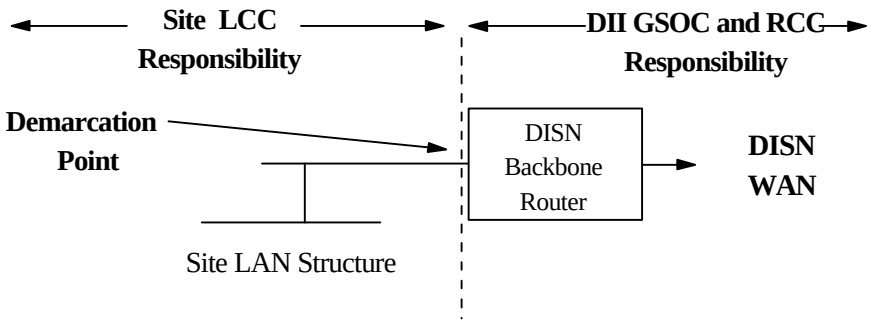

Figure 6: Demarcation Point of Responsibility for Ethernet Access to DISN Networks.

Figure 7 provides a logical demarcation representation for the physical demarcation show in Figure 5. The top portion of the drawing shows the seven layers of the Open Systems Interconnection (OSI) reference model for protocol definitions. Across the bottom of the drawing is a physical connectivity drawing similar to that of Figure 5. However, Figure 7 really shows two copies of Figure 5 back-to-back to show how a community-of-interest's site would be interlinked to another one of its site for example on the NIPRNET. In the middle of the drawing is the breakdown of who manages which portions of the link. The NIPRNET RCCs are responsible for their WAN routers and the access circuits to those routers. The local sites are responsible for their premise routers and their local site LANs. In most cases, communities of interest also have an overall management center operating out of some central location that has monitoring oversight for all of that community's functionality across the globe. This can be viewed as the central management location having oversight from the application on one end system to the application on another end system thus providing total asset viability.

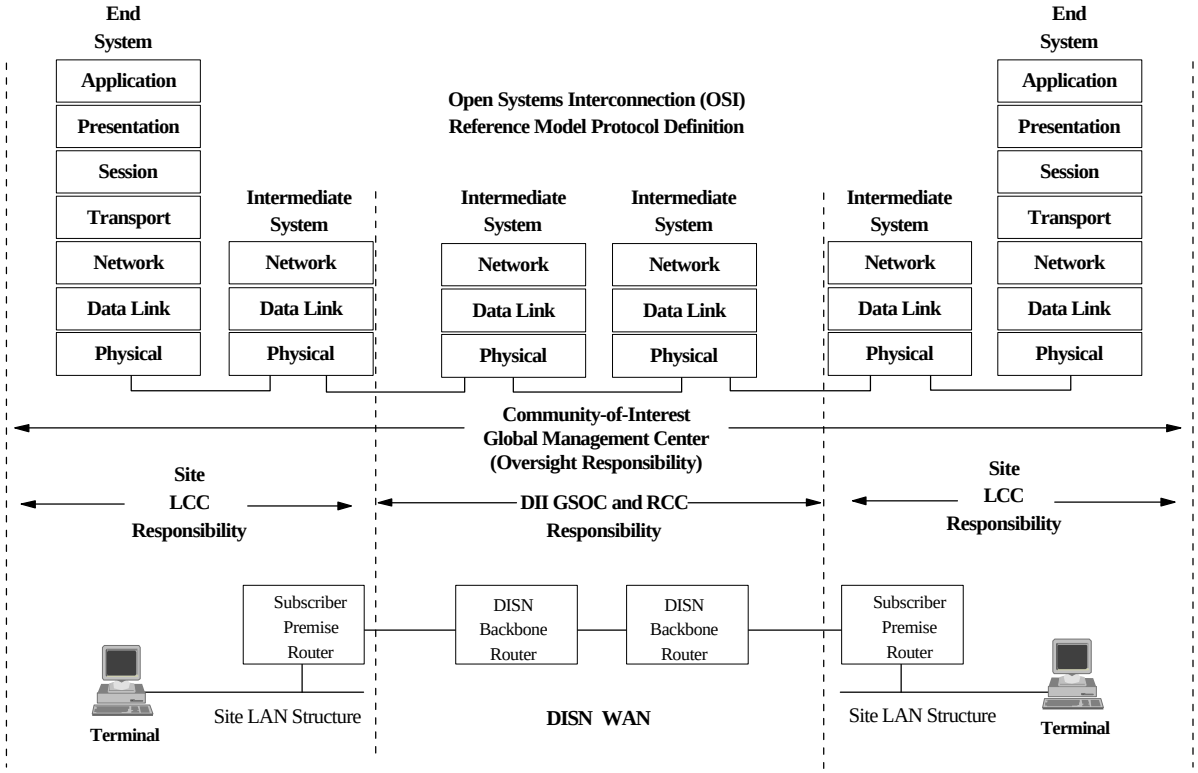

Figure 7: Logical Demarcation Points of Responsibility Based on OSI Protocol Model.

The previous diagrams reflect a pure demarcation between the DISN WANs and subscriber community locations. The DISN now offers management of customer premise equipment of a fee-for-service basis. The DISA/D343 office should be contacted for current information.

1.2.5 Service and Agency Wide Area Networks (WANs).

To be added later.

1.2.6 Specialized Metropolitan Wide Area Networks (MANs).

To be added later.

1.2.7 Base, Post, Campus Local Area Networks (LANs).

To be added later. Topics to cover will include; interoperability between LANs and WANS, influence of S/A policy on programs and networks, and the impact of specific S/A regulations.

1.2.8 Specific Systems or Programs Network Management Missions.

To be added later.

1.3 Document Overview.

This document outlines the software capabilities required for DII COE Network Management (NM) applications in accordance with the content and format guidance of *Software Requirements Specification (SRS), Data Item Description (DID), Identification Number: DI-IPSC-81433*.

- Section 1 identifies the scope and provides an overview of the DII COE.
- Section 2 lists the documents which are applicable to NM and are referenced in this document.
- Section 3 provides a list of functional capability requirements.
- Section 4 identifies the qualification provisions.
- Section 5 defines the traceability methodologies needed to account for Network Management requirements.
- Section 6 contains the applicable notes associated with DII COE Network Management.

Distribution of this entire document is authorized to U.S. Government Agencies and their contractors for critical technology as identified on the front cover. Further dissemination of this document will require written approval from the DISA DII COE Engineering Office. If the requirements traceability identified in section 5 is removed prior to distribution, then the modified document is approved for public release with unlimited distribution. Only the modified document missing section 5 will be posted on the NETTWG page of the DII COE HomePage. The web address is: http://spider.osfl.disa.mil/dii/aog_twg/twg/nmstwg/nmstwg_page.html.

2. Referenced Documents.

2.1 DOD and Federal Documents.

The following specifications, standards, and handbooks are used to varying degrees to build the foundation of this document. Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DoDISS) and supplements. Most of the public domain documentation can be obtained in electronic soft copy via anonymous ftp retrieval. When using anonymous ftp, login to the remote host as *anonymous* and use the password *anonymous*, *guest*, or your e-mail address. Specific password instructions usually are given during the login process. When possible, the remote host and path/filename are given for the documents listed below. Copies of these documents can be obtained from:

Documents Order Desk
Building 4D
700 Robbins Avenue
Philadelphia, PA 19111-5094

Copies of Federal Information Processing Standards (FIPS) and those documents published by the National Institute of Standards and Technology (NIST) may be obtained from:

National Technical Information Services (NTIS)
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

or:

Standards Office, NIST
Building 225, Room B64
Gaithersburg, MD 20899
(301) - 975-2816

Documents:

(1) Department of Defense, DOD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, 21 March 1988.

(2) Department of Defense, DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985 (Orange Book).

(3) FIPS Publication 179, *Government Network Management Profile (GNMP)*, 15 Dec. 92.
Electronic ftp retrieval

Remote host = osi.ncsl.nist.gov
Path/filename = pub/gnmp

(4) FIPS Publication 146-1, *Government Open Systems Interconnection Profile (GOSIP), Version 2.0*, 3 Apr. 91.
Electronic ftp retrieval
Remote host = osi.ncsl.nist.gov
Path/filename = pub/gosip

(5) *Industry/Government Open Systems Specifications (IGOSS), Version 1*, May 94.
Electronic ftp retrieval
Remote host = osi.ncsl.nist.gov
Path/filename = pub/igoss

(6) MIL-STD-2045-17507, *Internet Network Management Profile for DOD Communications, Parts 1-3*, DRAFT, 1 June 1994.

(7) MIL-HNBK-1351, *Network Management for DOD Communications*, 23 Jul. 93.

(8) NIST Special Publication 500-214, *Stable Implementation Agreements for Open Systems Interconnection Protocols, Open Systems Environment Implementors Workshop (OIW), Version 7, Edition 1*, Dec. 93.
Electronic ftp retrieval
Remote host = nemo.ncsl.nist.gov
Path/filename = pub/oiw/agreements/

(9) MIL-STD-2045-38000, *Network Management of DOD Communications*, DRAFT, 4 January 1993.

(10) Military STD.401, *Secure Data Network Systems (SDNS) Security Protocol 4 (SP4), Revision 1.3*, National Security Agency.

(11) NISTIR 4792, *A Formal Description of the SDNS Security Protocol at Layer 4 (SP4)*, Wayne Janse, Mar 92.

(12) *Department of Defense Technical Architecture Framework for Information Management, Version 2.0*, March 1995. OPR: DISA.
Electronic retrieval
www = http://www.itsi.disa.mil/cfs/tafim.html

(13) MIL-STD-498, *Software Development and Documentation*, 5 December 1994.

(14) MIL-STD-973, *Configuration Management*, 17 April 1992.

(15) Department of Defense, DOD Handbook 5200-H, *Department of Defense Handbook for Writing Classification Guidance*.

(16) Department of Defense, DOD Index 5200-I, *Index of Security Classification Guides*.

(17) Department of Defense, DOD Pamphlet 5200-PH, *A Guide to Marking Classified Documents*.

(18) CJCSI 6212.01, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 July 1993.

(19) Department of Defense, DOD Regulation 5200.1, *DOD Information Security Program*.

(20) Department of Defense, DOD Regulation 5200.2, *DOD Personnel Security Program*.

(21) Draft *System Engineering Guidelines for the Implementation of a Base-Level Network Control Center*, 30 December 1994. OPR: AFC4A/TNSCC, Scott AFB IL.

(22) CSC-STD-002-85, Department of Defense Password Management Guidelines, 12 April 1985.

(23) Department of Defense, DOD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992.

(24) Department of Defense, DOD Directive C-5200.5, *Communications Security (COMSEC)*, 21 April 1990.

(25) Department of Defense, DOD Directive C-5200.19, *Control of Compromising Emanations*, 23 February 1990.

(26) NTISSI No. 7000, *TEMPEST Countermeasures for Facilities*, 29 November 1993.

2.2 DISA Documents.

Copies of DII COE and most GCCS specific documents may be obtained directly from the NIPRNET. The DII COE HomePage can be accessed at http://spider.osfl.disa.mil/dii. The unclassified GCCS HomePage can be accessed at http://spider.osfl.disa.mil/. If a referenced document is not available in electronic downloadable form then one can submit an on-line request for the document on either of these two web sites. Please check the DII COE and GCCS document listings carefully though before entering an electronic document request. The DISA

Operational Support Facility (OSF) CM policy states that requests for documents will not be processed for those documents that are already available for downloading from the GCCS or DII COE HomePages. In the event one does not have NIPRNET access a written request can be sent to the addresses listed below for DII COE and GCCS documentation.

DISA
Configuration Management Department
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Requests for non-DII COE or non-GCCS documents should be sent to the Office of Primary Responsibility (OPR) identified for each of the other DISA documents. For those unfamiliar with DISA, please contact the DISA Public Affairs at (703) 607-6900 if further assistance is required.

(1) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specifications*, Version 2.0, 23 October 1995, CM-165-60-02.

(2) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specifications*, Version 3.0 DRAFT (NOTE: This does not yet supersede Version 2.0 as it has not yet been approved), January 1997, CM-165-60-03.

(3) *Configuration Management Software and Documentation Delivery Requirements* (NOTE: This is used for DII COE and GCCS deliveries to the DISA OSF), Version 2.0, 24 April 1997, CM-400-01-01.

(4) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Developer Documentation Requirements*, Version 1.0, 29 April 1997, CM-400-214-02.

(5) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Style Guide*, Version 2.0, 1 April 1996, CM-400-18-02.

(6) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline Specifications*, Version 3.0, 31 October 1996, CM-400-25-05.

(7) *Defense Information Infrastructure (DII) Common Operating Environment (COE) Baseline Specifications*, Version 3.1, 29 April 1997, CM-400-25-07.

(8) *Defense Information Infrastructure (DII) Common Operating Environment (COE) How To Segment Guide*, Version 4.0, 30 December 1996, CM-400-130-01.

(9) CJCSI 6721.01, *Global Command and Control Management Structure*, 18 February 1995.

(10) *Global Command and Control System, Concept of Operations (CONOPS)*, 11 April 1995. OPR: JCS/J36

(11) *Global Command and Control System, System and Network Management, Concept of Operations (CONOPS), Version 1.8.2*, 16 December 1996, CM-500-189-02, OPR: DISA/JEJ.

(12) *Global Command and Control System, Program Management Plan*, 29 March 1995. OPR: DISA/D23.

(13) Global Command and Control System, *Joint Integrated Logistics Support Plan*, 8 June 1995. OPR: DISA/D23.

(14) *Defense Information System Network, Integrated Tactical Strategic Data Networking (ITSDN), Internet Protocol Addressing Plan*, 24 June 1994. OPR: DISA/JIEO/JEEFE

(15) Draft *Defense Information System Network, Dial-In Data Services, Internet Protocol Addressing Plan*. OPR: DISA/JIEO/JEEFE

(16) *Defense Information System Network, Secret Internet Protocol Network (SIPRNET) Addressing Plan*. OPR: DISA/JIEO/JEEFE

(17) *Defense Information System Network, Secret Internet Protocol Network (SIPRNET) Router Architecture Plan*. OPR: DISA/JIEO/JEEFE

(18) DISA Circular 310-70-X, *Methods and Procedures, DII Control Centers*. OPR: DISA/D5

(19) DISA Technical Report 93-07-C, *Joint Task Force Communications Planning and Management Concept of Operations, Final Report.* OPR: DISA/JIEO/JEEPB

(20) CJCSM 6231 *Employment of Joint Tactical Communications Systems, Volume 7, Network Management*. OPR: Joint Staff/J-6

(21) DISA/JIEO Report 8125, *Joint Task Force Tactical Communications Architecture*, March 1995. OPR: DISA/JIEO

2.3 Industry Standards.

Industry standards are developed by the International Standards Organization (ISO) and the International Telecommunications Union - Technology Sector (ITU-TS) formerly known as the International Telegraph and Telephone Consultative Committee (CCITT).

In addition to the above industry standards, the Network Management Forum has developed a set of pertinent specifications. The following documents are available from:

Network Management Forum (NMF)
1201 Mt. Kemble Avenue
Morristown, NJ 07960-6628

Documents:

(1) *OMNIPoint 1 Specifications*, 1993, and OMNIPoint 1+, 1994.

(2) *Service Provider Integrated Requirements for Information Technology (SPIRIT)*, Issue 2.0, 1994.

(3) Network Management Forum: Forum 026, *Translation of Internet MIBs to ISO/CCITT Guidelines for the Definition of Managed Objects (GDMO) Management Information Bases (MIBs)*, Issue 1.0, Oct. 93.

(4) Network Management Forum: Forum 027, *ISO/CCITT to Internet Management Security*, Issue 1.0, Oct. 93.
Electronic ftp retrieval
Remote host = thumper.bellcore.com
Path/filename = pub/forum/iimc/

(5) Network Management Forum: Forum 028, *ISO/CCITT to Internet Management Proxy*, Issue 1.0, Oct. 93.
Electronic ftp retrieval
Remote host = thumper.bellcore.com
Path/filename = pub/forum/iimc/

(6) Network Management Forum: Forum 029, *Translation of Internet MIB-II (RFC-1213) to ISO/CCITT GDMO MIB*, Issue 1.0, Oct. 93.
Electronic ftp retrieval
Remote host = thumper.bellcore.com
Path/filename = pub/forum/iimc/

(7) Network Management Forum: Forum 030, *Translation of ISO/CCITT GDMO MIBs to Internet MIBs*, Issue 1.0, Oct. 93.
Electronic ftp retrieval
Remote host = thumper.bellcore.com
Path/filename = pub/forum/iimc/

2.4 Internet Publications.

An Internet Architecture Board (IAB) standard is published as an IAB STD. An IAB standard is published as a Request for Comment (RFC) document. In addition to the RFCs listed below, draft and proposed RFCs are developed and distributed for comments. RFC 1500 is an index to all RFCs. These documents are available from:

DOD Network Information Center
7990 Boeing Court
MS CV-50
Vienna, VA 22183-7000
Toll-free: 1-800-365-3642
International: 1-703-821-6266
Web Site: http://nic.ddn.mil/
Unclass e-mail: nic@nic.ddn.mil

Electronic retrievals of RFCs are from the same remote host, ds.internic.net, and the path/filename is rfc####.txt where #### is the 4-digit RFC number.

Documents:

(1) RFC 1500, *Internet Official Protocol Standards*, Aug. 93.

(2) RFC 1155, *Structure of Management Information (SMI)*, May 90.

(3) IAB STD 15 (RFC 1157), *Simple Network Management Protocol (SNMP)*, May 90.

(4) RFC 1212, *Concise MIB Definitions*.

(5) IAB STD 17 (RFC 1213), *Management Information Base - II (MIB-II)*, Mar 91.

(6) RFC 1271, *Remote Monitoring Management Information Base (RMON MIB)*, Nov. 91.

(7) RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*, Apr. 93.

(8) RFC 1442, *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(9) RFC 1443, *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(10) RFC 1444, *Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(11) RFC 1445, *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(12) RFC 1446, *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(13) RFC 1447, *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(14) RFC 1448, *Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(15) RFC 1449, *Textual Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(16) RFC 1450, *Management Information Base of version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr. 93.

(17) RFC 1451, *Manager-to-Manager Management Information Base*, Apr. 93.

(18) RFC 1452, *Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework*, Apr. 93.

2.5 Order of Precedence.

In the event of a conflict between the text of this document and the documents cited herein, the text of this document takes precedence. However, nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained. Please contact the chairperson of the DII COE NETTWG if further clarification is required.

3. Requirements.

3.1 Required States and Modes.

The Network Management functional area of the DII COE has no operating modes or states of its own since the DII COE is a foundation. However, DII COE-compliant systems do have various modes of operation. The four general modes are:

Operational Mode: This is the normal mode of operation where the DII COE-compliant system is on-line supporting the operational mission of the community of interest.

Maintenance Mode: In this mode, portions of the hardware or software associated with a DII COE-compliant system at a particular site will be off-line for maintenance, modification, upgrade, or other related actions.

Training Mode: In this mode, a portion of the DII COE-compliant system may be operating with separate databases using simulated inputs in support of training for a portion of the user population of the community of interest. Care must be taken to ensure that exercise data is not mixed with operational data.

Exercise Mode: In this mode, a portion of the DII COE-compliant system may be operated with separate databases using simulated inputs in support of an exercise for a portion of the user population of the community of interest. This could be for war gaming purposes or for testing new functionalities for the community of interest.

It is important to understand these modes of operation are not mutually exclusive. In fact, normal day-to-day operations will probably find all four operating modes existing at the same time within different portions of a large-scale DII COE-compliant system. The different modes will be distinguished by administrative features, geographical or architectural boundaries, or management domains. The Network Management functional area requirements are valid for all required states and modes.

3.2 Network Management (NM) Functional Area Capability Requirements.

This section describes the various requirements for the network management capabilities to be available in DII COE-compliant network management applications. The requirements are based on two primary sources. The first sources of requirements are the published documents pertaining to network management such as MIL-STD-2045-38000 (Network Management for DOD Communications), MIL-HDBK-1351 (Network Management for DOD Communications), and FIPS Publication 179-1 (Government Network Management Profile (GNMP)). The other sources of requirements are those that come from the various DII COE user community developers and chief engineers that build end systems. Twice a year the DII COE Engineering

Office conducts a formal requirements call for DII COE capabilities. This call goes out through the voting members of the DII COE Architecture Oversight Group (AOG). Requirements can also be submitted out-of-cycle through the appropriate TWG provided the voting member of the AOG for that Service or Agency approves the submission. For more information on the DII COE schedule consult the COE Engineering Page off of the DII COE HomePage.

This section captures all validated network management requirements submitted to the DII COE Engineering Office through the NETTWG. Overall, each TWG is responsible for tracking and maintaining the requirements for their functional areas. The network management requirements are subdivided into various classifications with a further subdivision into categories. This breakdown and functional grouping of network management requirements will help the reader better comprehend the organization of Section 3.2. The six primary classifications of requirements are listed below. Each will be explained in more detail later. They are:

- Management Architecture.
- Management Components.
- Management Applications.
- Management System Characteristics.
- Security for Management Operations.
- Coexistence of OSI-Based and IPS-Based NM Technologies.

All of the tables within Section 3.2 stating requirements follow the same five-column format. The first column provides a unique paragraph number that must always be referenced when changes are recommended to existing requirements. All new requirements submitted to the NETTWG will be sorted and assigned paragraph numbers as required. This does not, however, prevent the submitter of requirements from providing a recommendation as to which section the requirement belongs in. The second column is the description of the requirement. The requirement must be clearly and completely described in words that can be understood by nontechnical individuals. The NETTWG will work with the submitter to ensure the requirements are properly understood and captured. The third column identifies the DII COE version in which the capability is required. Consult the DII COE HomePage if further detailed scheduling information is required. The fourth column identifies which operating systems, supported by the DII COE Engineering Office, the capability is required for. This column does not specifically address a particular version of an operating system because this is explicitly identified by the DII COE version number. Here it is sufficient to specify Solaris (Sol), Hewlett Packard (HP), or Microsoft NT (NT). The final column is for comments. This column will be used to record the source of the requirement. Those entries with an NETTWGYYMMDD-XXX designation represent the date the NETTWG revalidated requirements that were contained in either the *Software Requirements Specification (SRS) for the Defense Information Infrastructure (DII) Common Operating Environment (COE) for Platform Services* document or the *Software Requirements Specification for the Network Administration Functional Area of the Global Command and Control System (GCCS)* document. In some cases the “Comments” column contains a reference like “NM.GEN.3.2.1" or

"NM.SYS.000" in the field. This reference traces back to the GCCS SRS document. Those GCCS SRS requirements with a "000" reference number indicate those that did not make it into the consolidated SRS because of an administrative oversight. Both full sets of requirements were worked by the NETTWG to ensure the most complete set of legacy requirements. Other entries in the "Comments" field capture the source and date of newer requirements submitted to the DII COE Engineering Office. Organizations who submitted requirements but do not see them listed in this document must work through their Service or Agency representative to the NETTWG to resolve the issue.

3.2.1 Management Architecture.

The management architecture section deals with the extremely high level requirements of the most basic nature for network management functionality. This includes requirements as basic as "network management will exist" or that "a NM database will exist" for supporting the network management applications. Others are that NCCs will exist and objects will be managed using the MIBs. Again, these are high-level requirements that will satisfy basic programmatic needs. More detailed requirements will be captured the more detailed sections that follow.

3.2.1.1 General Architecture Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.1.1	NM shall be provided.	3.1+	Sol/HP/NT	NETTWG970321-1 NM.GEN.3.2.1
3.2.1.1.2	NM shall be interoperable with the goals and structure of the DII.	3.1+	Sol/HP/NT	NETTWG970321-2 NM.GEN.3.2.2
3.2.1.1.3	Industry standard, object-oriented, distributed systems architectures (as identified in current and future OMNIPoint specifications) shall be used to support installation and interoperability of distributed DII NM applications.	3.1+	Sol/HP/NT	NETTWG970321-3 NM.ARCH.3.2.1.1
3.2.1.1.4	The three types of logical management components or services (i.e., managed systems, manager systems, and management gateways) shall support the following Functional Management Areas (FMAs) as partitioned by the ISO: configuration management, fault management, performance management, accounting management, and security management.	3.1+	Sol/HP/NT	NETTWG970321-4 NM.ARCH.3.2.1.2
3.2.1.1.5	Multiple managers, multiple managed systems, and multiple management gateways shall be integrated so as to allow common observation and control of the composite of completely dissimilar logical and physical resources/services.	3.1+	Sol/HP/NT	NETTWG970321-5 NM.ARCH.3.2.1.3

3.2.1.1.6	NM systems may be capable of supporting two types of management information pools: (1) databases (both integrated and non-integrated) and (2) Management Information Bases (MIBs).	3.1+	Sol/HP/NT	NETTWG970321-6 NM.ARCH.3.2.1.4
3.2.1.1.7	NM shall scale to a complex enterprise.	4.0	NT	Health Affairs NM 14 16 May 1997
	End			

Table 3.2.1.1: General Architecture Requirements.

3.2.1.2 Database Architecture Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.2.1	Management databases shall be capable of being distributed in order to meet database robustness requirements affected by communication outage characteristics.	3.1+	Sol/HP/NT	NETTWG970321-7 NM.ARCH.000
3.2.1.2.2	Management databases shall be capable of maintaining critical parameter values (e.g., defaults) locally.	3.1+	Sol/HP/NT	NETTWG970321-8 NM.ARCH.000
3.2.1.2.3	Management databases shall be able to retain dynamic, static, status, and statistical information.	3.1+	Sol/HP/NT	NETTWG970321-9 NM.ARCH.000
3.2.1.2.4	Management databases shall conform to the data elements and fields as defined in the Defense Data Repository System (DDRS) whenever possible.	3.1+	Sol/HP/NT	NETTWG970321-10 NM.ARCH.000
3.2.1.2.5	Management applications that use application-specific data elements and fields shall be held to a minimum or avoided completely.	3.1+	Sol/HP/NT	NETTWG970321-11 NM.ARCH.000
3.2.1.2.6	Management databases shall be capable of being accessed unambiguously.	3.1+	Sol/HP/NT	NETTWG970321-12 NM.ARCH.000
3.2.1.2.7	Management databases shall be capable of being manipulated, subject to relevant security policies, by database management systems (DBMSs).	3.1+	Sol/HP/NT	NETTWG970321-13 NM.ARCH.000
	End			

Table 3.2.1.2: Database Architecture Requirements.

3.2.1.3 Management Information Base (MIB) Architecture Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.1.3.1	Management system components/services shall have a common understanding of management information databases and MIBs, access characteristics, and the structure of managed objects.	3.1+	Sol/HP/NT	NETTWG970321-14 NM.ARCH.3.2.1.5
3.2.1.3.2	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the best estimate of the total number of collisions of a given Ethernet segment (etherStatsCollisions) for remote monitoring.	3.1+	Sol/HP/NT	NETTWG970321-15 NM.ARCH.3.2.1.6
3.2.1.3.3	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the total number of events in which packets were dropped by the probe due to lack of resources during a given interval (not necessarily the number of packets dropped, but the number of occurrences) (etherHistoryDropEvents) for remote monitoring.	3.1+	Sol/HP/NT	NETTWG970321-16 NM.ARCH.3.2.1.6
3.2.1.3.4	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the best estimate of the mean physical layer network utilization of a given interface during a given interval (in hundredths of a percent) (etherHistoryUtilization) for remote monitoring.	3.1+	Sol/HP/NT	NETTWG970321-17 NM.ARCH.3.2.1.6
3.2.1.3.5	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the threshold for a given sampled statistic (when the current sampled value is greater than or equal to a specified threshold, and the value of the last sampling interval was less than a specified threshold, a single event shall be generated) (alarmRisingThreshold) for remote monitoring.	3.1+	Sol/HP/NT	NETTWG970321-18 NM.ARCH.3.2.1.6
3.2.1.3.6	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include a list of top N host control entries (hostTopNControlTable) for remote monitoring.	3.1+	Sol/HP/NT	NETTWG970321-19 NM.ARCH.3.2.1.6

3.2.1.3.7	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the amount of time since a given host was last initialized (hrSystemUptime) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-20 NM.ARCH.3.2.1.7
3.2.1.3.8	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the number of user sessions for which a given host is storing system information (hrSystemNumUsers) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-21 NM.ARCH.3.2.1.7
3.2.1.3.9	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the number of process contexts currently loaded or running on the system (hrSystemProcesses) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-22 NM.ARCH.3.2.1.7
3.2.1.3.10	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the amount of physical main memory contained by a given host (hrMemorySize) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-23 NM.ARCH.3.2.1.7
3.2.1.3.11	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the size of storage represented by a given entry (hrStorageSize) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-24 NM.ARCH.3.2.1.7
3.2.1.3.12	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the current operational state of a given device (hrDeviceStatus) for host resource monitoring purposes.	3.1+	Sol/HP/NT	NETTWG970321-25 NM.ARCH.3.2.1.7
3.2.1.3.13	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include a table describing currently running processes on the node in which a given SNMP agent resides (processTable) for other resources.	3.1+	Sol/HP/NT	NETTWG970321-26 NM.ARCH.3.2.1.8

3.2.1.3.14	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the accumulated CPU time for a given process (in seconds) (processTime) for other resources.	3.1+	Sol/HP/NT	NETTWG970321-27 NM.ARCH.3.2.1.8
3.2.1.3.15	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the errors reported to the system console (errorTable) for other resources.	3.1+	Sol/HP/NT	NETTWG970321-28 NM.ARCH.3.2.1.8
3.2.1.3.16	The management information that can be shared among managed systems, manager systems, and management gateways within a domain, as well as the types of management information that is to be made available to other management domains, shall include the percentage of a device's total capacity in use (devCapacity) for other resources.	3.1+	Sol/HP/NT	NETTWG970321-29 NM.ARCH.3.2.1.8
	End			

Table 3.2.1.3: Management Information Base (MIB) Architecture Requirements.

3.2.1.4 Network Control Center (NCC) Architecture Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.1.4.1	Overall management responsibility in a domain shall be assigned to a logical Network Control Center (NCC).	3.1+	Sol/HP/NT	NETTWG970321-30 NM.ARCH.3.2.1.11
3.2.1.4.2	A NCC shall coordinate NM functions within its domain of jurisdiction and between its domain and other domains.	3.1+	Sol/HP/NT	NETTWG970321-31 NM.ARCH.3.2.1.11
3.2.1.4.3	A NCC shall have appropriate managed system, manager system, and management gateway capabilities to allow it to interact with, and pass appropriate management information and commands among NM components/services in its own and other domains.	3.1+	Sol/HP/NT	NETTWG970321-32 NM.ARCH.3.2.1.11
3.2.1.4.4	Allocations and reallocations of resources to domains, as well as managers to domains, shall be capable of being made dynamically according to a variety of factors (including at least the following: ownership, mission, mission function, organization, geography, administration, accounting, technology, equipment or resource or resource service type being managed, performance requirements, management policy, and security policy).	3.1+	Sol/HP/NT	NETTWG970321-33 NM.ARCH.3.2.1.12

3.2.1.4.5	Domains shall be capable of being partitioned into multiple subordinate domains, each of which may have its own manager.	3.1+	Sol/HP/NT	NETTWG970321-34 NM.ARCH.3.2.1.13
3.2.1.4.6	Each management domain shall be able to accommodate more than one manager system managing resources within the domain.	3.1+	Sol/HP/NT	NETTWG970321-35 NM.ARCH.3.2.1.13
3.2.1.4.7	Overall management responsibility in a domain shall be capable of being assigned to a logical NCC.	3.1+	Sol/HP/NT	NETTWG970321-36 NM.ARCH.3.2.1.13
3.2.1.4.8	A peer NCC, designated as a backup, be able to serve as the hot backup for any other NCC within that management domain.	3.1+	Sol/HP/NT	NETTWG970321-37 NM.ARCH.3.2.1.15
3.2.1.4.9	A scheme or sequence of hot backups shall be able to be put in place for extremely critical NCCs or for specific, extremely critical, NCC functionality.	3.1+	Sol/HP/NT	NETTWG970321-38 NM.ARCH.3.2.1.15
3.2.1.4.10	A hot backup capability is required for peer NCCs.	3.1+	Sol/HP/NT	NETTWG970321-39 NM.ARCH.3.2.1.15
3.2.1.4.11	To the maximum extent possible, an NCC shall use Open Systems Interconnection (OSI) specified systems management protocols, functions, services, and information.	3.1+	Sol/HP/NT	NETTWG970321-40 NM.ARCH.3.2.1.17
3.2.1.4.12	An NCC shall be able to provide summary management information and/or significant summary event reports to other NCCs, managers, and/or management gateways.	3.1+	Sol/HP/NT	NETTWG970522-1 NM.COMP.000
3.2.1.4.13	An NCC shall be able to provide detailed management information and/or significant summary event reports about its own domain to other NCCs, or to managers and/or management gateways within its domain of jurisdiction.	3.1+	Sol/HP/NT	NETTWG970522-2 NM.COMP.000
3.2.1.4.14	An NCC shall be able to provide on-line management policy and security policy information from hierarchically, higher-level NCCs to neighboring (peer) NCCs, to NCCs of any hierarchically, lower-level management domain, and to managers or management gateways within its domain of jurisdiction.	3.1+	Sol/HP/NT	NETTWG970522-3 NM.COMP.000
	End			

Table 3.2.1.4: Network Control Center (NCC) Architecture Requirements.

3.2.2 Management Components.

The network management components are the basic building blocks that make up the overall NM architecture. The components are broken into several different categories. The NM components include sections on protocols, manager systems and management gateways. NCC component requirements are also captured. The NM components may exist as logical capabilities within other devices, resources or services. Management components also may exist as standalone, separately accessible devices or services. Two subcategories of NM protocols exist, those managed items based on Open Systems Interconnection (OSI) standards and those items based on

Internet Protocol Suite (IPS) standards. The following sections identify the DII COE network management component requirements.

3.2.2.1 General Component Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.1.1	The DII COE Network Management products shall provide Ada interfaces (e.g., Ada bindings) for all public APIs.	3.1+	Sol/HP/NT	AFATDS.NET.1 16 May 1997
3.2.2.1.2	NM shall provide APIs which permit easy and flexible extensions to management.	4.0	NT	Health Affairs NM 19 16 May 1997
	End			

Table 3.2.2.1: General Component Requirements.

3.2.2.2 Protocol Component Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.2.1	OSI-based NM components shall utilize the standard management communication protocols as stipulated in the OMNIPoint specifications such as SNMP and CMIP.	3.1+	Sol/HP/NT	NETTWG970424-1 NM.COMP.000
3.2.2.2.2	IPS-based NM components shall utilize the standard management communication protocols of the Internet management communication protocol, SNMP, OMNIPoint 1, and/or OMNIPoint 1+.	3.1+	Sol/HP/NT	NETTWG970424-2 NM.COMP.000
3.2.2.2.3	Manager systems components shall include multiple management technologies (i.e., a manager shall have OSI-based management capabilities and IPS-based management capabilities IAW the GNMP and OMNIPoint 1 and OMNIPoint 1+).	3.1+	Sol/HP/NT	NETTWG970424-3 NM.COMP.000
3.2.2.2.4	NM shall support SNMP v1.0.	4.0	NT	Health Affairs NM 16 16 May 1997
3.2.2.2.5	NM shall support SNMP v2.0.	4.0	NT	Health Affairs NM 17 16 May 1997
3.2.2.2.6	NM shall provide support for discovery of other level-III protocols like AppleTalk, IPX, etc.	4.0	NT	Health Affairs NM 23 16 May 1997
	End			

Table 3.2.2.2: Protocol Component Requirements.

3.2.2.3 Gateway Component Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.3.1	Each NCC shall be able to function as a management gateway.	3.1+	Sol/HP/NT	NETTWG970424-4 NM.COMP.000
3.2.2.3.2	Gateways between Internet and OSI management paradigms shall be IAW OMNIPoint 1 or the IGOSS specification. (Note: These ISO/Internet Management coexistence specifications provide mappings between Internet communication protocols (SNMPv1 and SNMPv2) and OSI management communication protocols as well as mappings between OSI Structure of Management Information (SMI) and Internet SMI, as well as translations of certain MIBs.)	3.1+	Sol/HP/NT	NETTWG970424-5 NM.COMP.000
3.2.2.3.3	The specifications and implementation agreements pertinent to OSI/IPS-based management gateway capabilities shall be those that appear in the NMF Forum documents and the OIW Agreements. (Note: The OIW agreements, Part 18, Annex E, provides detailed management information definitions associated with numerous Internet-to-OSI translated MIBs. This document also identifies and provides references to other Internet-to-OSI translated MIBs.)	3.1+	Sol/HP/NT	NETTWG970424-6 NM.COMP.000
3.2.2.3.4	An OSI/IPS management gateway shall be used when an OSI-based management system and IPS-based management system must interact to exchange manager-to-manager or manager-to integrator information.	3.1+	Sol/HP/NT	NETTWG970618-8 NM.COMP.000
	End			

Table 3.2.2.3: Gateway Component Requirements.

3.2.2.4 Manager System Component Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.4.1	The ability to build NM command files and to load new managed object definitions without re-compiling management applications shall be provided in manager systems to the network administrator.	3.1+	Sol/HP/NT	NETTWG970424-14 NM.SYS.000
3.2.2.4.2	The ability to perform a remote login to remote manager systems shall be supported in accordance with an identity-based security policy.	3.1+	Sol/HP/NT	NETTWG970424-15 NM.SYS.000

3.2.2.4.3	Manager systems (including generic manager systems called management platforms) shall include standard Application Programming Interfaces (APIs), such as those identified in current or future OMNIPoint specifications.	3.1+	Sol/HP/NT	NETTWG970522-4 NM.COMP.000
3.2.2.4.4	The exchange of management commands and information among remote management entities shall not degrade significantly the aggregate quality of the services provided by managed resources to end users of those resources.	3.1+	Sol/HP/NT	NETTWG970522-5 NM.COMP.000
3.2.2.4.5	When management communication traffic occurs in dedicated channels that are not in-band with end-user traffic, the management traffic shall be constrained to fit within its dedicated channel capacity allocation and the time delay constraints.	3.1+	Sol/HP/NT	NETTWG970522-6 NM.COMP.000
3.2.2.4.6	Performance requirements pertaining to NM processing speeds and capacities, the minimum number of transactions that can be processed by all manager systems shall be no less than 400 per minute.	3.1+	Sol/HP/NT	NETTWG970522-7 NM.APPS.000
3.2.2.4.7	A multiple protocol stack manager system shall provide a common API that allows management applications to have ready use of both underlying OSI-based and IPS-based management technologies.	3.1+	Sol/HP/NT	NETTWG970522-153 NM.APPS.000
3.2.2.4.8	The management technology and infrastructure, the management communication protocols, and the management information associated with all newly-acquired manager systems shall be upgradeable readily via convenient software upgrade capabilities and via easy driver hardware swaps.	3.1+	Sol/HP/NT	NETTWG970522-154 NM.APPS.000
3.2.2.4.9	A multiple protocol stack management system shall be used to manage a hybrid network (i.e., a network which includes both OSI-based and IPS-based components).	3.1+	Sol/HP/NT	NETTWG970618-9 NM.COMP.000
3.2.2.4.10	NM shall support multiple client workstations.	4.0	NT	Health Affairs NM 13 16 May 1997
	End			

Table 3.2.2.4: Manager System Component Requirements.

3.2.2.5 Network Control Center (NCC) Component Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.2.5.1	No requirements exist for this section at this time			
	End			

Table 3.2.2.5: Network Control Center (NCC) Component Requirements.

3.2.3 Management Applications.

This section deals with specific NM application functionality that is required. This section does not capture the interaction between applications. It is strictly for the pure, internal requirements of the NM applications. In almost all cases the requirements in this section will be satisfied by commercial products. The following sections represent the initial list of NM applications. It is likely that additional NM applications will be defined as NM application requirements are submitted through future requirements calls. New applications will be appended to the end of this section.

3.2.3.1 General Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.1.1	OSI-based NM applications shall support standard management ensembles as appropriate (e.g., those identified in the current or future OMNIPoint specifications and/or DOD management ensembles.).	3.1+	Sol/HP/NT	NETTWG970424-7 NM.APPS.000
3.2.3.1.2	NM applications shall be able to support the installation and execution of portable management applications across all management system platforms within the domain.	3.1+	Sol/HP/NT	NETTWG970424-8 NM.APPS.000
3.2.3.1.3	NM applications shall be able to share their management information repositories and to support common management operations upon such repositories.	3.1+	Sol/HP/NT	NETTWG970424-9 NM.APPS.000
3.2.3.1.4	NM applications shall include management information development and maintenance tools applications.	3.1+	Sol/HP/NT	NETTWG970424-10 NM.APPS.000
3.2.3.1.5	NM applications shall include integrated alarm reporting and trouble tracking applications.	3.1+	Sol/HP/NT	NETTWG970424-11 NM.APPS.000
3.2.3.1.6	NM applications shall include change and inventory control management applications.	3.1+	Sol/HP/NT	NETTWG970424-12 NM.APPS.000
3.2.3.1.7	NM applications shall include training aids applications.	3.1+	Sol/HP/NT	NETTWG970424-13 NM.APPS.000
3.2.3.1.8	NM shall provide separation of management console(s), management server, and management agents in a client-server approach.	4.0	NT	Health Affairs NM 12 16 May 1997
	End			

Table 3.2.3.1: General Application Requirements.

3.2.3.2 HelpDesk/Trouble-Ticketing Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.3.2.1	Any failures of alarm/trouble ticket activities within network-administrator-specified time durations shall result in an alarm that shall require network administrator intervention.	3.1+	Sol/HP/NT	NETTWG970424-45 NM.SYS.000
3.2.3.2.2	The automatically closing of trouble tickets upon successful verification shall be archived together with related fault correction information as specified by the network administrator (e.g., a list of actions taken to remedy the situation).	3.1+	Sol/HP/NT	NETTWG970522-65 NM.SYS.000
3.2.3.2.3	The occupance of closing security attack trouble tickets shall be archived together with related security attack correction information (e.g., a list of actions taken to remedy the situation) as specified by the network/security administrator.	3.1+	Sol/HP/NT	NETTWG970522-138 NM.SEC.000
3.2.3.2.4	NM shall provide for third party trouble ticket systems.	4.0	NT	Health Affairs NM 26 16 May 1997
	End			

Table 3.2.3.2: HelpDesk/Trouble-Ticketing Application Requirements.

3.2.3.3 Change/Inventory Control Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.3.1	The NM system shall update administrator-specified configuration records pertinent to those resources as specified by the network administrator .	3.1+	Sol/HP/NT	NETTWG970522-34 NM.SYS.000
3.2.3.3.2	IRT to accounting management, the NM system shall have the capability to inform network administrator and users of costs incurred or resources used (e.g., budgeting, billing verification, cost estimation for proposed configurations, internal cost allocation, customer billing, etc.).	3.1+	Sol/HP/NT	NETTWG970522-94 NM.SEC.000
	End			

Table 3.2.3.3: Change/Inventory Control Application Requirements.

3.2.3.4 Remote Monitoring Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.4.1	No requirements exist for this section at this time			
	End			

Table 3.2.3.4: Remote Monitoring Application Requirements.

3.2.3.5 Simple Network Manager Protocol (SNMP) Manager Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.5.1	The NM system shall be able to control, directly and dynamically, remote configurable resources (e.g.; multiplexers; routers; switches; frequency-setable, bandwidth-setable or time-slot-setable radios; etc.).	3.1+	Sol/HP/NT	NETTWG970522-24 NM.SYS.000
3.2.3.5.2	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to establishing, maintaining or altering configuration, topology, and state of the manageable resources.	3.1+	Sol/HP/NT	NETTWG970522-25 NM.SYS.000
3.2.3.5.3	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to the startup and shutdown of manageable resources.	3.1+	Sol/HP/NT	NETTWG970522-26 NM.SYS.000
3.2.3.5.4	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to the reconstitution of manageable resources.	3.1+	Sol/HP/NT	NETTWG970522-27 NM.SYS.000
3.2.3.5.5	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to the correction of faults in managed resources.	3.1+	Sol/HP/NT	NETTWG970522-28 NM.SYS.000
3.2.3.5.6	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to the performance tuning of managed resources.	3.1+	Sol/HP/NT	NETTWG970522-29 NM.SYS.000
3.2.3.5.7	IAW the GNMP, NM manager systems, managed systems and management gateways shall have the capability to remotely create/delete attributes and to remotely modify individual or administrator-selectable groups of attributes pertinent to altering accounting algorithms based on actual resources used.	3.1+	Sol/HP/NT	NETTWG970522-30 NM.SYS.000
3.2.3.5.8	NM shall provide or support a MIB browser.	4.0	NT	Health Affairs NM 18 16 May 1997
	End			

Table 3.2.3.5: SNMP Manager Application Requirements.

3.2.3.6 Network Topology/Mapping Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.6.1	A NM system application for network topology map editing shall have the capability to create, label, modify, geographically locate, manipulate, rotate, size, save, recall and reuse, cut and paste, and delete network topology map icons.	3.1+	Sol/HP/NT	NETTWG970424-58 NM.SYS.000
3.2.3.6.2	A NM system application for network topology map editing shall have the capability to create, modify, geographically locate, manipulate, rotate, size, group, save, recall and reuse, cut and paste, and delete sets of icons onto existing or other network topology maps.	3.1+	Sol/HP/NT	NETTWG970424-59 NM.SYS.000
3.2.3.6.3	A NM system application for network topology map editing shall have the ability to move/rotate an icon or group of icons, while retaining a connection representation between the icon/icon-group and a fixed location on a network topology map.	3.1+	Sol/HP/NT	NETTWG970424-60 NM.SYS.000
3.2.3.6.4	A NM system application for network topology map editing shall have the ability to input scanned graphical images (e.g., maps, photo graphics, etc.).	3.1+	Sol/HP/NT	NETTWG970424-61 NM.SYS.000
3.2.3.6.5	NM shall allow the arrangement of discovered entities in a given view and group entities into different hierarchical levels.	4.0	NT	Health Affairs NM 3 16 May 1997
3.2.3.6.6	NM shall allow addition of new entities manually and relate them to discovered ones.	4.0	NT	Health Affairs NM 4 16 May 1997
	End			

Table 3.2.3.6: Network Topology/Mapping Application Requirements.

3.2.3.7 Report Generation Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.7.1	No requirements exist for this section at this time			
	End			

Table 3.2.3.7: Report Generation Application Requirements.

3.2.3.8 Capacity/Bandwidth Utilization Application Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.3.8.1	The COE shall provide a GUI that displays external communications throughput information. The term "external communications" shall represent terrestrial and satellite communications bandwidth trunks in support of JWICS, SIPRNET, NIPRNET, and similar DOD WAN and MAN architectures. The terms shall also represent low-speed modem bandwidths, e.g., 9.6Kbps terrestrial modem, and radio line of sight (LOS) bandwidth connections from remote stationary or portable sites to a JWICS, SIPRNET, or NIPRNET node.	4.0	Sol/HP/NT	DoDIIS-N-44 16 May 1997
	End			

Table 3.2.3.7: Report Generation Application Requirements.

3.2.4 Management System Characteristics.

NM system characteristics deal with how the architectural components along with the specific NM applications must all interact. This section defines the requirements relationships between those two major areas. It is imperative that sound human engineering factors are used throughout the management system. This will enable operators to rapidly comprehend and use the capabilities provided. NM analysis tools must be able to provide several different types of predetermined, preprogrammed and/or new, ad-hoc, on-demand information reports. These analysis tools shall include mechanisms that enable the appropriate tool(s) and report(s) to be selected by the network administrator during online NM operations. The following are DII COE NM system characteristic requirements.

3.2.4.1 General System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.1.1	The management system shall be able to scale the management capabilities it makes available to each specific network administrator automatically.	3.1+	Sol/HP/NT	NETTWG970424-21 NM.SYS.000
3.2.4.1.2	The scaling of management capabilities shall be based on the access privileges or type of network administrator using the management system.	3.1+	Sol/HP/NT	NETTWG970424-22 NM.SYS.000
3.2.4.1.3	The NM system shall be able to support applications that pertain to disaster preparedness planning as well as to disaster recovery (e.g., with respect to fire, flood, etc.) by storage of online configuration and management data at an off-site location.	3.1+	Sol/HP/NT	NETTWG970424-46 NM.SYS.000

3.2.4.1.4	NM shall support user customizable interface (e.g., it should be possible to add a new menu item, execute a custom-built program, etc.).	4.0	NT	Health Affairs NM 8 16 May 1997
3.2.4.1.5	NM shall support fault-tolerant operation in the event of a server failure.	4.0	NT	Health Affairs NM 15 16 May 1997
3.2.4.1.6	NM shall provide support for backup and archiving.	4.0	NT	Health Affairs NM 28 16 May 1997
3.2.4.1.7	NM shall provide support and management capability for hierarchical storage.	4.0	NT	Health Affairs NM 29 16 May 1997
	End			

Table 3.2.4.1: General System Requirements.

3.2.4.2 Automated Processes System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.2.1	Automatic fault and performance NM applications shall have the ability to automatically issue a trouble ticket and/or multiple, cross-referenced trouble tickets to initiate appropriate repair/replace actions.	3.1+	Sol/HP/NT	NETTWG970424-43 NM.SYS.000
3.2.4.2.2	Trouble tickets shall be cleared automatically after automated testing is used subsequently to assure that repair/replace activities have been successfully completed, and that a given resource or service is ready to be restored.	3.1+	Sol/HP/NT	NETTWG970424-44 NM.SYS.000
	End			

Table 3.2.4.2: Automated Processes System Requirements.

3.2.4.3 Autodiscovery System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.3.1	NM shall enable the system configuration monitoring operations (used in conjunction with all appropriate NM components) to identify the physical devices (routers, bridges, hubs, etc.) that comprise a network.	3.1+	Sol/HP/NT	NETTWG970522-9 NM.SYS.000
3.2.4.3.2	NM shall enable the system configuration monitoring operations (used in conjunction with all appropriate NM components) to assess the configuration, characteristics and state of manageable physical devices or NM applications.	3.1+	Sol/HP/NT	NETTWG970522-10 NM.SYS.000

3.2.4.3.3	NM shall enable the system configuration monitoring operations (used in conjunction with all appropriate NM components) to assess the relationships among manageable physical devices and among other manageable physical devices, services, and NM applications.	3.1+	Sol/HP/NT	NETTWG970522-11 NM.SYS.000
3.2.4.3.4	NM information shall be obtained via automatic, auto-discovery mechanisms.	3.1+	Sol/HP/NT	NETTWG970522-14 NM.SYS.000
3.2.4.3.5	It shall be possible for the network administrator to enter manually or to override manually, management information associated with automatic autodiscovery processes.	3.1+	Sol/HP/NT	NETTWG970522-15 NM.SYS.000
3.2.4.3.6	All manual override actions associated with the automatic autodiscovery processes shall cause the generation of an appropriate event, including before and after images of the changed management information, to be entered into a log and/or audit trail record.	3.1+	Sol/HP/NT	NETTWG970522-16 NM.SYS.000
3.2.4.3.7	All new configuration information and statistics gathered from automatic autodiscovery processes shall update any NM databases archiving current and historical static resource/service configuration information.	3.1+	Sol/HP/NT	NETTWG970522-17 NM.SYS.000
3.2.4.3.8	NM shall support node discovery at any pre-determined time of a specific network. Note: Health Affairs NM 2 was split into three different requirements.	4.0	NT	Health Affairs NM 2 16 May 1997
3.2.4.3.9	NM shall support node discovery at any pre-determined time a group of devices in the specified range of addresses. Note: Health Affairs NM 2 was split into three different requirements.	4.0	NT	Health Affairs NM 2 16 May 1997
3.2.4.3.10	NM shall support node discovery at any pre-determined time a specific device. Note: Health Affairs NM 2 was split into three different requirements.	4.0	NT	Health Affairs NM 2 16 May 1997
3.2.4.3.11	NM shall provide user defined polling interval, the ability to turn the polling of an entity on or off for a specified time interval, and to revert to the previous state after that interval has elapsed.	4.0	NT	Health Affairs NM 7 16 May 1997
	End			

Table 3.2.4.3: Autodiscovery System Requirements.

3.2.4.4 Alarm Generation System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.4.4.1	It shall be possible for alarms from a variety of network-administrator-selectable management entities to be forwarded to network-administrator-specified NM applications invoked to isolate the problems and to diagnose their source(s) and cause(s) in order to minimize the need for human intervention.	3.1+	Sol/HP/NT	NETTWG970424-42 NM.SYS.000
3.2.4.4.2	The NM system shall support an alarm presentation capability where posted alarms shall correspond to a similar color icon in the presentation pane.	3.1+	Sol/HP/NT	NETTWG970618-1 NM.COEX.000
3.2.4.4.3	The NM system shall support an alarm presentation capability where the system shall distinguish between acknowledged and unacknowledged alarm messages.	3.1+	Sol/HP/NT	NETTWG970618-2 NM.COEX.000
3.2.4.4.4	The NM system shall support an alarm presentation capability where the system shall permit a user to simultaneously accept all assigned alarms.	3.1+	Sol/HP/NT	NETTWG970618-3 NM.COEX.000
3.2.4.4.5	The NM system shall support an alarm presentation capability where each alarm acknowledgment shall be logged automatically along with the identification of the user.	3.1+	Sol/HP/NT	NETTWG970618-4 NM.COEX.000
3.2.4.4.6	The NM system shall support an alarm presentation capability where the audit trail shall contain system receive time, assignee, acknowledgment, if responsibility is declined, and time cleared.	3.1+	Sol/HP/NT	NETTWG970618-5 NM.ARCH.000
3.2.4.4.7	The NM system shall support an alarm presentation capability where the alarm disposition shall be maintained via an audit trail.	3.1+	Sol/HP/NT	NETTWG970618-6 NM.ARCH.000
3.2.4.4.8	The NM system shall support an alarm presentation capability where the system shall be able to poll periodically, on a scheduled basis, for alarms, events, and status messages.	3.1+	Sol/HP/NT	NETTWG970618-7 NM.ARCH.000
3.2.4.4.9	NM shall provide user defined control of which devices and MIB variables are monitored, their relative importance, which alerts are critical and the action to be taken on each alarm.	4.0	NT	Health Affairs NM 6 16 May 1997
3.2.4.4.10	NM shall provide alert notifications via graphical icons and colors.	4.0	NT	Health Affairs NM 21 16 May 1997
3.2.4.4.11	NM shall provide alert notifications via touch-tone or alphanumeric pagers.	4.0	NT	Health Affairs NM 24 16 May 1997
	End			

Table 3.2.4.4: Alarm Generation System Requirements.

3.2.4.5 Report Generation System Requirements.

The report generation requirements are subdivided into additional sections to make it easier to track the requirements. The subsections are: report output requirements, report tools requirements, and report algorithm requirements.

3.2.4.5.1 Report Output Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.5.1.1	The NM system shall collect, process, and format management data into Network Administrator specified formatted outputs (e.g., graphs, bar charts, maps, audible alarms, voice-annotated reports, etc.).	3.1+	Sol/HP/NT	NETTWG970424-16 NM.SYS.000
3.2.4.5.1.2	The network administrator shall be able to request and/or select whether each predetermined and/or ad hoc information report is to be made available in response to an ad hoc query from the network administrator, or whether it is to be automatically reported periodically.	3.1+	Sol/HP/NT	NETTWG970424-28 NM.SYS.000
3.2.4.5.1.3	For reports that are to be reported periodically, the network administrator shall be able to specify the starting date/time and/or the event that triggers the start of automatic reporting.	3.1+	Sol/HP/NT	NETTWG970424-29 NM.SYS.000
3.2.4.5.1.4	For reports that are to be reported periodically, the network administrator shall be able to specify the ending date/time and/or the event that triggers the cessation of automatic reporting.	3.1+	Sol/HP/NT	NETTWG970424-30 NM.SYS.000
3.2.4.5.1.5	For reports that are to be reported periodically, the network administrator shall be able to specify the time interval between reports and/or the event that shall trigger individual reports during a period of automatic reporting.	3.1+	Sol/HP/NT	NETTWG970424-31 NM.SYS.000
3.2.4.5.1.6	The network administrator shall be able to dynamically create summary reports of specified events (e.g., fault detection, configuration status, performance degradations, security events, etc.).	3.1+	Sol/HP/NT	NETTWG970424-32 NM.SYS.000
3.2.4.5.1.7	The network administrator shall be able to dynamically create summary reports of specified events sorted by criteria that are specifiable and selectable by the network administrator.	3.1+	Sol/HP/NT	NETTWG970424-33 NM.SYS.000
3.2.4.5.1.8	The network administrator shall be able to dynamically create summary reports of automatically recognized new event patterns and/or situations that may need to be monitored.	3.1+	Sol/HP/NT	NETTWG970424-34 NM.SYS.000
3.2.4.5.1.9	The network administrator shall be able to dynamically create summary reports of network-administrator-selectable threshold limits that are exceeded.	3.1+	Sol/HP/NT	NETTWG970424-35 NM.SYS.000
3.2.4.5.1.10	The network administrator shall be able to dynamically create summary reports of traffic loads and patterns of current characteristics and historical trends of systems control and management traffic (e.g., duty cycle, inter-arrival characteristics, volume, type of message/protocol, etc.).	3.1+	Sol/HP/NT	NETTWG970424-36 NM.SYS.000

3.2.4.5.1.11	The network administrator shall be able to dynamically create summary reports of traffic loads and patterns of aggregated link/channel statistics.	3.1+	Sol/HP/NT	NETTWG970424-37 NM.SYS.000
3.2.4.5.1.12	The network administrator shall be able to dynamically create summary reports of resources' availability, status, operational MTTF/MTBF/MTTR characteristics, remaining mean time duration to expected failure, remaining mean time to scheduled preventative maintenance.	3.1+	Sol/HP/NT	NETTWG970424-38 NM.SYS.000
3.2.4.5.1.13	The network administrator shall be able to dynamically create summary reports of system-wide network-administrator-selectable logical and physical resources (e.g., circuits) indicating network-administrator-selectable features (e.g., identify active links, failed links, overloaded links, geographic and logical location, etc.).	3.1+	Sol/HP/NT	NETTWG970424-39 NM.SYS.000
3.2.4.5.1.14	The network administrator shall be able to dynamically create summary reports of network-administrator-selectable elements (e.g., the boards, available slots, bus structure, software) associated with each piece of managed equipment, and network-administrator-selectable features of these elements and/or equipment (e.g., logical and physical resources to which items are connected logically and physically).	3.1+	Sol/HP/NT	NETTWG970424-40 NM.SYS.000
3.2.4.5.1.15	The network administrator shall be able to dynamically create summary reports of path tracings between logical and physical resources (including alternate paths with network-administrator-selectable features).	3.1+	Sol/HP/NT	NETTWG970424-41 NM.SYS.000
3.2.4.5.1.16	The mean acceptable time delay for the manager system to complete processing any individually requested summary report shall be 5 minutes.	3.1+	Sol/HP/NT	NETTWG970522-8 NM.APPS.000
3.2.4.5.1.17	The NM system shall be able to present fault-related information, as specified or selected by the network administrator, to network-administrator-specified or selected destinations (e.g., a network administrator's display/monitoring screen, a local information store, an end user of a specific individual resource/service or of a specific class of resources/services; a remote management information data base, etc.).	3.1+	Sol/HP/NT	NETTWG970522-74 NM.SYS.000
3.2.4.5.1.18	NM shall provide user defined & formatted reports.	4.0	NT	Health Affairs NM 20 16 May 1997
	End			

Table 3.2.4.5.1: Report Output Requirements.

3.2.4.5.2 Report Tools Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.4.5.2.1	The NM administrator shall be able to select the criteria upon which pre-programmed and ad hoc, on-demand, real-time, and historical outputs can be created.	3.1+	Sol/HP/NT	NETTWG970424-17 NM.SYS.000
3.2.4.5.2.2	Network administrators shall be able to control which NM information and/or category of information shall be capable of being output (e.g., all information pertinent to administrator-specified management domains or manager systems).	3.1+	Sol/HP/NT	NETTWG970424-18 NM.SYS.000
3.2.4.5.2.3	Network administrators shall be able to control which logical and/or physical device NM information is outputted to.	3.1+	Sol/HP/NT	NETTWG970424-19 NM.SYS.000
3.2.4.5.2.4	Network administrators shall be able to control in which format NM Information is to be outputted in (e.g., display screens, windows, storage devices, help desks, groups of remote managers or managed systems, printers, etc.).	3.1+	Sol/HP/NT	NETTWG970424-20 NM.SYS.000
3.2.4.5.2.5	Automated analysis tools shall be available to create several different types of pre-determined/pre-programmed information reports that are capable of being selected by the network administrator during live management operations.	3.1+	Sol/HP/NT	NETTWG970424-23 NM.SYS.000
3.2.4.5.2.6	Automated analysis tools shall be able to create new, ad hoc, on-demand information reports as specified by the network administrator.	3.1+	Sol/HP/NT	NETTWG970424-24 NM.SYS.000
3.2.4.5.2.7	The Network Administrator shall be able to generate ad hoc information reports using a variety of tools and/or software algorithms/modules that are resident natively and/or inputted by the Network Administrators (e.g., ad hoc, general-purpose data reduction, data selection/filtering, data transformation, ensemble-oriented and time-series-oriented statistical analysis, statistical inference, expert system, pattern recognition/analysis, artificial intelligence, report writing, graphical display, and fuzzy logic tools).	3.1+	Sol/HP/NT	NETTWG970424-25 NM.SYS.000
3.2.4.5.2.8	The tools and algorithms shall be capable of being applied to any network-administrator-selected management information.	3.1+	Sol/HP/NT	NETTWG970424-26 NM.SYS.000
3.2.4.5.2.9	Any parameters and other features of automated analysis tools and algorithms shall be capable of being input and/or selected by the network administrator during live operations.	3.1+	Sol/HP/NT	NETTWG970424-27 NM.SYS.000
	End			

Table 3.2.4.5.2: Report Tools Requirements.

3.2.4.5.3 Report Algorithm Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.5.3.1	No requirements exist for this section at this time			
	End			

Table 3.2.4.5.3: Report Algorithm Requirements.

3.2.4.6 Modeling and Simulation System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.6.1	The NM system shall have the capability to model and simulate new networks and applications or changes to existing configurations in order to predict the impact and results (e.g., optimization of assets for least cost provisioning, integral network mapping, design tools with access to tariffs and existing configurations, usage trend analysis, and traffic and load projections of new objects).	3.1+	Sol/HP/NT	NETTWG970522-93 NM.SEC.000
	End			

Table 3.2.4.6: Modeling and Simulation System Requirements.

3.2.4.7 Resource Monitoring System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.7.1	NM shall enable the system configuration monitoring operations (used in conjunction with all appropriate NM components) to assess performance characteristics of manageable physical devices, services, and NM applications.	3.1+	Sol/HP/NT	NETTWG970522-12 NM.SYS.000
3.2.4.7.2	NM shall enable the system configuration monitoring operations (used in conjunction with all appropriate NM components) to assess NM performance monitoring capabilities.	3.1+	Sol/HP/NT	NETTWG970522-13 NM.SYS.000
3.2.4.7.3	The network administrators shall be able through scheduling and event reporting capabilities to identify which CM information is to be examined or tracked.	3.1+	Sol/HP/NT	NETTWG970522-18 NM.SYS.000
3.2.4.7.4	The network administrators shall be able through scheduling and event reporting capabilities to identify the method by which CM information is to be obtained (e.g., polling, event-driven reports, etc.).	3.1+	Sol/HP/NT	NETTWG970522-19 NM.SYS.000

3.2.4.7.5	The network administrators shall be able through scheduling and event reporting capabilities to identify the schedule by which CM information is to be obtained, (i.e., the start and stop date/time of configuration monitoring operations, and the frequency of obtaining CM information when configuration monitoring operations are enabled).	3.1+	Sol/HP/NT	NETTWG970522-20 NM.SYS.000
3.2.4.7.6	The network administrators shall be able through scheduling and event reporting capabilities to identify which management events are to be reported.	3.1+	Sol/HP/NT	NETTWG970522-21 NM.SYS.000
3.2.4.7.7	The network administrators shall be able through scheduling and event reporting capabilities to identify the destination(s) to which each management event is to be reported.	3.1+	Sol/HP/NT	NETTWG970522-22 NM.SYS.000
3.2.4.7.8	The network administrators shall be able through scheduling and event reporting capabilities to identify the criteria that must be met to send management events.	3.1+	Sol/HP/NT	NETTWG970522-23 NM.SYS.000
3.2.4.7.9	The NM system shall monitor and estimate unused resource capacity margins to those resources as specified by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-31 NM.SYS.000
3.2.4.7.10	The NM system shall schedule and de-schedule the allocation of unused resource capacity pertinent to those resources as specified by the network administrator .	3.1+	Sol/HP/NT	NETTWG970522-32 NM.SYS.000
3.2.4.7.11	The NM system shall be able to observe one or more performance-related variables which are associated with one or more managed objects.	3.1+	Sol/HP/NT	NETTWG970522-85 NM.SYS.000
3.2.4.7.12	The NM system shall be able to make performance-related observations via ensemble sampling (i.e., by observing across several instances of managed resources/services at the same network-administrator-selected time).	3.1+	Sol/HP/NT	NETTWG970522-86 NM.SYS.000
3.2.4.7.13	The NM system shall be able to make performance-related observations via time-series sampling (i.e., by observing a single network-administrator-selectable managed resource/service at network-administrator-setable, uniformly-spaced-in-time, observation (sampling) times).	3.1+	Sol/HP/NT	NETTWG970522-87 NM.SYS.000
3.2.4.7.14	The NM system shall be able to make performance-related observations via historical sampling (i.e., by recalling previous performance observations stored in a log and/or a performance information buffer).	3.1+	Sol/HP/NT	NETTWG970522-88 NM.SEC.000
3.2.4.7.15	IRT performance testing, the NM system shall be able to conduct confidence tests on network-administrator-selected resources/services as well as performance tests on network-administrator-selected resources/services.	3.1+	Sol/HP/NT	NETTWG970522-91 NM.SEC.000
3.2.4.7.16	IRT performance testing, all supported confidence and performance tests shall include the ability to undertake network-administrator-controlled, artificially-generated traffic that feature network-administrator-setable traffic characteristics.	3.1+	Sol/HP/NT	NETTWG970522-92 NM.SEC.000
3.2.4.7.17	The COE shall provide a GUI that displays network throughput information.	4.0	Sol/HP/NT	DoDIIS-N-36 16 May 1997

	End			

Table 3.2.4.7: Resource Monitoring System Requirements.

3.2.4.8 Logs/Audit Trail System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.8.1	A NM system application shall have the capability to initiate, terminate, suspend, and resume the activity of logging and/or auditing management event reports.	3.1+	Sol/HP/NT	NETTWG970424-52 NM.SYS.000
3.2.4.8.2	A NM system application shall have the capability to allocate the size of a specific log and/or audit trail.	3.1+	Sol/HP/NT	NETTWG970424-53 NM.SYS.000
3.2.4.8.3	A NM system application shall have the capability to manually search and view logged event types, log attribute values, notifications of log attribute value changes, managed objects, and/or management information/attributes contained within audit trails, logs and MIBs.	3.1+	Sol/HP/NT	NETTWG970424-54 NM.SYS.000
3.2.4.8.4	A NM system application shall have the capability to automatically search a specified audit trail, log and/or MIB according to user-definable, ad hoc, mnemonic search keys, and to identify automatically and to make available for viewing, and as appropriate for manipulation, specified logged event types, log attribute values, notifications of log attribute value changes, managed objects, and/or management information/attributes.	3.1+	Sol/HP/NT	NETTWG970424-55 NM.SYS.000
3.2.4.8.5	A NM system application shall have the capability to automatically search a specified audit trail, log and/or MIB according to user-definable, ad hoc, correlation criteria and to identify automatically and to make available for viewing, and as appropriate for manipulation, correlated logged event types, log attribute values, notifications of log attribute value changes, managed objects, and/or management information/attributes.	3.1+	Sol/HP/NT	NETTWG970424-56 NM.SYS.000
3.2.4.8.6	A NM system application shall have the capability to archive and/or delete user-specifiable logged event types, log attribute values, notifications of log attribute value changes, managed objects, and/or management information/attributes from an active audit trail, log and/or MIB.	3.1+	Sol/HP/NT	NETTWG970424-57 NM.SYS.000
	End			

Table 3.2.4.8: Logs/Audit Trail System Requirements.

3.2.4.9 Fault System Requirements.

The fault requirements are subdivided to additional sections to make it easier to track the requirements. The subsections are: fault analysis requirements, fault correlation requirements, fault correction requirements, fault prevention requirements, and fault history requirements.

3.2.4.9.1 Fault Analysis Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.9.1.1	IRT fault detection, resource monitoring capabilities shall be used in conjunction with all NM components to schedule and to execute the monitoring of resources for fault indications.	3.1+	Sol/HP/NT	NETTWG970522-39 NM.SYS.000
3.2.4.9.1.2	IRT fault cause analysis, the NM system shall be able to analyze fault indications using techniques as well as time series analysis and statistical ensemble analysis, to determine root causes of problems to within statistical inference and hypothesis testing accuracy measures (i.e., false positive rates and false negative rates).	3.1+	Sol/HP/NT	NETTWG970522-40 NM.SYS.000
3.2.4.9.1.3	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to identify redundant and/or correlated fault indications.	3.1+	Sol/HP/NT	NETTWG970522-41 NM.SYS.000
3.2.4.9.1.4	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to set thresholds to block redundant/correlated fault indications, or to examine situations with greater resolution and/or granularity.	3.1+	Sol/HP/NT	NETTWG970522-42 NM.SYS.000
3.2.4.9.1.5	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to use alarm correlation tools to estimate most likely root causes of failures.	3.1+	Sol/HP/NT	NETTWG970522-43 NM.SYS.000
3.2.4.9.1.6	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to identify the existence of faults during conditions when conflicting fault indications or observations about the state of resources exist.	3.1+	Sol/HP/NT	NETTWG970522-44 NM.SYS.000
3.2.4.9.1.7	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to verify the existence of faults using on-demand, direct inquiries of, and tests of, suspicious components, resources, and services, as well as the neighboring components, resources, and services to such suspicious elements.	3.1+	Sol/HP/NT	NETTWG970522-45 NM.SYS.000
3.2.4.9.1.8	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to characterize identified faults in terms of network-administrator-specified/selected parameters (e.g., fault persistence, correlated factors, general geographic location of the offending resource at which the fault exists (to within an administrator-selectable location granularity), precise logical/physical location of fault (to within an administrator-selectable granularity), etc.).	3.1+	Sol/HP/NT	NETTWG970522-46 NM.SYS.000

3.2.4.9.1.9	IRT fault cause analysis, the NM system analysis capabilities shall have the ability to use pattern analysis techniques to learn of new events and situations to be monitored, and to modify fault detection mechanisms to accommodate and to use such new events and situations to detect new and different types of fault indications.	3.1+	Sol/HP/NT	NETTWG970522-47 NM.SYS.000
3.2.4.9.1.10	The NM system shall have the ability to verify fault correction through on-demand, network-administrator-selectable testing.	3.1+	Sol/HP/NT	NETTWG970522-62 NM.SYS.000
3.2.4.9.1.11	The NM system on-demand, network-administrator-selectable testing shall be able to assure that a given resource or service is ready to be restored and that repair/replace activities have been successfully completed.	3.1+	Sol/HP/NT	NETTWG970522-63 NM.SYS.000
3.2.4.9.1.12	The NM system on-demand, network-administrator-selectable testing shall automatically close associated trouble tickets upon successful verification that a faulty resource/service has been restored.	3.1+	Sol/HP/NT	NETTWG970522-64 NM.SYS.000
3.2.4.9.1.13	NM shall provide fault notifications via e-mail to users.	4.0	NT	Health Affairs NM 5 16 May 1997
	End			

Table 3.2.4.9.1: Fault Analysis Requirements.

3.2.4.9.2 Fault Correlation Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.9.2.1	IRT fault management control, the NM system shall be able to control fault monitoring activities, fault testing activities, fault-related thresholds, and fault testing/correction.	3.1+	Sol/HP/NT	NETTWG970522-83 NM.SYS.000
3.2.4.9.2.2	The NM system shall be able to detect and to characterize normal and degraded performance of managed resources/services, as well as the characteristics of traffic offered to and/or delivered by such resources/services.	3.1+	Sol/HP/NT	NETTWG970522-84 NM.SYS.000
	End			

Table 3.2.4.9.2: Fault Correlation Requirements.

3.2.4.9.3 Fault Correction Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.4.9.3.1	IRT fault correction initiation decision-making, the NM system shall have automated abilities to continually analyze fault determinations and recommend decisions as to whether or not to initiate corrective actions on a determined fault.	3.1+	Sol/HP/NT	NETTWG970522-48 NM.SYS.000
3.2.4.9.3.2	IRT fault correction initiation decision-making, the complexity characteristics of decision criteria for initiating fault correction activities shall include the ability to trigger a decision based on appropriate factors from the fault correction policy established by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-49 NM.SYS.000
3.2.4.9.3.3	IRT fault correction actions, the NM system shall have the ability to change, reset and/or reboot attribute values associated with manageable resources/services as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-50 NM.SYS.000
3.2.4.9.3.4	IRT fault correction actions, the NM system shall have the ability to switch to redundant resources/services as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-51 NM.SYS.000
3.2.4.9.3.5	IRT fault correction actions, the NM system shall have the ability to circumvent faulty resources/services by switching to alternative resources/services which may not be exactly functionally equivalent to, or may not have the exact same performance characteristics of, the faulty resource/service as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-52 NM.SYS.000
3.2.4.9.3.6	IRT fault correction actions, the NM system shall have the ability to disable faulty resources/services as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-53 NM.SYS.000
3.2.4.9.3.7	IRT fault correction actions, the NM system shall have the ability to isolate faulty resources/services from the operational network by disabling all links that attach to the faulty resource/service so as to prevent spread of outages/faults to other resources (e.g., as in the case with faults caused by roving viruses) as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-54 NM.SYS.000
3.2.4.9.3.8	IRT fault correction actions, the NM system shall have the ability to request manual replacement of faulty resources/services as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-55 NM.SYS.000
3.2.4.9.3.9	IRT fault correction actions, the NM system shall have the ability to request on-line or off-line repair of faulty resources/services as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-56 NM.SYS.000
3.2.4.9.3.10	IRT fault correction actions, the NM system shall have the ability to open trouble/repair ticketing and tracking activities on the faulty resource/service and associated work order tickets as selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-57 NM.SYS.000
3.2.4.9.3.11	IRT fault correction actions, the NM system shall include the ability to execute a sequence of one or more actions to be applied to faulty resources or to be requested of providers of faulty services:	3.1+	Sol/HP/NT	NETTWG970522-58 NM.SYS.000
3.2.4.9.3.12	IRT fault correction tracking, the NM system shall have the ability to track the status of on-line corrective actions as well as off-line repair activities.	3.1+	Sol/HP/NT	NETTWG970522-59 NM.SYS.000

3.2.4.9.3.13	IRT fault correction tracking, the NM system shall have the ability to provide estimates of the expected time to complete resource/service restoral.	3.1+	Sol/HP/NT	NETTWG970522-60 NM.SYS.000
3.2.4.9.3.14	IRT fault correction tracking, the NM system shall have the ability to provide estimates of the expected time to return to full survivability levels.	3.1+	Sol/HP/NT	NETTWG970522-61 NM.SYS.000
3.2.4.9.3.15	The complexity characteristics of decision criteria for initiating fault correction activities shall include at least the ability to trigger a decision based on a single threshold such as one representing a setable ratio of a resource/service time-in-use measure to the expected MTBF measure.	3.1+	Sol/HP/NT	NETTWG970522-82 NM.SYS.000
	End			

Table 3.2.4.9.3: Fault Correction Requirements.

3.2.4.9.4 Fault Prevention Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.9.4.1	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as scheduling routine confidence and preventative maintenance tests.	3.1+	Sol/HP/NT	NETTWG970522-75 NM.SYS.000
3.2.4.9.4.2	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as executing routine confidence and preventative maintenance tests.	3.1+	Sol/HP/NT	NETTWG970522-76 NM.SYS.000
3.2.4.9.4.3	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as developing archives of confidence and preventative maintenance test results.	3.1+	Sol/HP/NT	NETTWG970522-77 NM.SYS.000
3.2.4.9.4.4	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as notifying end users of resources/services of resource/service testing that will happen or that is happening.	3.1+	Sol/HP/NT	NETTWG970522-78 NM.SYS.000
3.2.4.9.4.5	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as determining actual, observed fault characteristics of specific categories of fielded resources/services from test results archives and fault correction archives.	3.1+	Sol/HP/NT	NETTWG970522-79 NM.SYS.000

3.2.4.9.4.6	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as exercising fault correction activities, upon network administrator approval, on specific individual resources/services that have time-in-use characteristics surpassing administrator-setable criteria based on vendor-quoted and/or actual historically observed MTTF or MTBF values that apply to specific classes of resources/services.	3.1+	Sol/HP/NT	NETTWG970522-80 NM.SYS.000
3.2.4.9.4.7	The NM system shall be capable of being directed by the network administrator to undertake selectable fault prevention activities such as exercising fault correction activities, upon network administrator approval, on specific individual resources/services for which network-administrator-setable criteria have been exceeded with respect to trends of increased incidences of network-administrator-setable anomalies or fault transients.	3.1+	Sol/HP/NT	NETTWG970522-81 NM.SYS.000
	End			

Table 3.2.4.9.4: Fault Prevention Requirements.

3.2.4.9.5 Fault History Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.9.5.1	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include reports of information about when an individual resource/service will resume operation after a failure has been detected.	3.1+	Sol/HP/NT	NETTWG970522-66 NM.SYS.000
3.2.4.9.5.2	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include reports of profiles estimating when specific resources/services will require preventative testing and when specific resources/services will require preventative fault correction actions (such estimation algorithms shall be based on predictions of expected mean time duration to expected failure and expected mean time to scheduled maintenance).	3.1+	Sol/HP/NT	NETTWG970522-67 NM.SYS.000
3.2.4.9.5.3	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include archives of results of all confidence and diagnostic tests.	3.1+	Sol/HP/NT	NETTWG970522-68 NM.SYS.000

3.2.4.9.5.4	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include archives of occurrences of faults of specific instances of resources/services, including the conditions of surrounding and associated resources/services, as well as the sequence of effective (and ineffective) corrective actions taken.	3.1+	Sol/HP/NT	NETTWG970522-69 NM.SYS.000
3.2.4.9.5.5	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include archives of time-in-use data for network-administrator-specified individual resources/services.	3.1+	Sol/HP/NT	NETTWG970522-70 NM.SYS.000
3.2.4.9.5.6	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include archives of actual time durations for the time-to-first failure, the time-between-successive-failures, and time-to-repair for each individual resource/service in a class of resources/services selected by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-71 NM.SYS.000
3.2.4.9.5.7	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include reports of actual or observed MTTF, MTBF, and MTTR statistics for network-administrator-selected classes of resources/services based on archives of specific values of appropriate, observed time durations for individual instances of resources/services in the class of resources/services.	3.1+	Sol/HP/NT	NETTWG970522-72 NM.SYS.000
3.2.4.9.5.8	The NM system shall report and archive fault information including fault indications, fault determinations, fault diagnosis, fault correction plans, and fault correction/repair status, to include accounting credit/rebate information pertinent to bad or unavailable services.	3.1+	Sol/HP/NT	NETTWG970522-73 NM.SYS.000
	End			

Table 3.2.4.9.5: Fault History Requirements.

3.2.4.10 Training System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.10.1	A NM system application shall have the capability to provide detailed, on-line, computer based training courses and demonstrations that are tailorable to the level of background of the individual being trained.	3.1+	Sol/HP/NT	NETTWG970424-47 NM.SYS.000
	End			

Table 3.2.4.10: Training System Requirements.

3.2.4.11 Help Function System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.11.1	A NM system application shall have the capability to provide detailed on-line, on-request, help instructions that are tailorable to the level of experience of the network administrator and that can provide information about, and procedures associated with, the NM system as a whole as well each NM application and each capability/operation within the NM system and/or each NM application.	3.1+	Sol/HP/NT	NETTWG970424-48 NM.SYS.000
3.2.4.11.2	A NM system application shall have the capability to provide the ability to automatically recognize, during operations, what the experience level of the network administrator is and, as needed, to provide additional, on-line guidance (in the extreme without the network administrator's manual request for such help) on how to proceed with the NM application being used by the network administrator.	5.0	Sol/HP/NT	NETTWG970424-49 NM.SYS.000
3.2.4.11.3	A NM system application shall have the capability to provide detailed on-line help text information related to specific alarm points.	3.1+	Sol/HP/NT	NETTWG970424-50 NM.SYS.000
3.2.4.11.4	A NM system application shall have the capability to provide text-based searching in the help function.	3.1+	Sol/HP/NT	NETTWG970424-51 NM.SYS.000
	End			

Table 3.2.4.11: Help Function System Requirements.

3.2.4.12 Capacity/Bandwidth Management System Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.4.12.1	The NM system shall allocate and de-allocate resource capacity that becomes available pertinent to those resources as specified by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-33 NM.SYS.000

3.2.4.12.2	The NM system shall identify the need to procure or to provision additional communications service capacity pertinent to those resources as specified by the network administrator.	3.1+	Sol/HP/NT	NETTWG970522-35 NM.SYS.000
3.2.4.12.3	The NM system shall provide dynamic, near real-time, capacity allocation tools (i.e., to handle traffic surges, such as experienced during regional conflicts, and natural and man-made disasters) to estimate unused resource capacity.	3.1+	Sol/HP/NT	NETTWG970522-36 NM.SYS.000
3.2.4.12.4	The NM system shall provide dynamic, near real-time, capacity allocation tools (i.e., to handle traffic surges, such as experienced during regional conflicts, and natural and man-made disasters) to track and analyze resource traffic loading characteristics.	3.1+	Sol/HP/NT	NETTWG970522-37 NM.SYS.000
3.2.4.12.5	The NM system shall provide dynamic, near real-time, capacity allocation tools (i.e., to handle traffic surges, such as experienced during regional conflicts, and natural and man-made disasters) to configure existing resources or to deny/delay access to resource usage based on any priority/precedence levels assigned to traffic.	3.1+	Sol/HP/NT	NETTWG970522-38 NM.SYS.000
3.2.4.12.6	The NM system shall be able observe one or more traffic characterization variables that are associated with one or more managed objects.	3.1+	Sol/HP/NT	NETTWG970522-89 NM.SEC.000
3.2.4.12.7	The NM system shall be able to make traffic characterization observations either via ensemble sampling, via time-series sampling, or via historical sampling.	3.1+	Sol/HP/NT	NETTWG970522-90 NM.SEC.000
3.2.4.12.8	The COE shall provide a GUI that displays network throughput information.	4.0	Sol/HP/NT	DoDIIS-N-36 16 May 1997
3.2.4.12.9	The COE shall be configurable to logoff low priority user(s) when network throughput reaches n percent of available bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-37 16 May 1997
3.2.4.12.10	The default low bandwidth n shall be set to 90 percent.	4.0	Sol/HP/NT	DoDIIS-N-38 16 May 1997
3.2.4.12.11	The COE shall send a notification to user(s) who have been preempted for low available bandwidth. The notification will be sent n minutes before the user(s) applications are closed and they are logged off. NOTE: Two DoDISS-N-39 entries submitted to DISA.	4.0	Sol/HP/NT	DoDIIS-N-39 16 May 1997
3.2.4.12.12	The default user notification n shall be 5 minutes. NOTE: Two DoDISS-N-39 entries submitted to DISA.	4.0	Sol/HP/NT	DoDIIS-N-39 16 May 1997
3.2.4.12.13	The COE Consolidated Application Server (CAS) shall send a final 45 second notification to user(s) who will be logged off due to low available bandwidth. NOTE: Consolidated Application Server (CAS) identified in DoDISS-N-19.	4.0	Sol/HP/NT	DoDIIS-N-40 16 May 1997
3.2.4.12.14	The COE CAS shall logoff low priority user(s) due to low available bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-41 16 May 1997
3.2.4.12.15	The COE shall send an alert to the network administrator(s) and system administrator(s) when average used bandwidth reaches n percent of available bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-42 16 May 1997

3.2.4.12.16	The default average used bandwidth shall be 85 percent.	4.0	Sol/HP/NT	DoDIIS-N-43 16 May 1997
3.2.4.12.17	The COE shall be configurable to logoff low priority user(s) when external communications throughput reaches n percent of available bandwidth. The term "external communications" shall represent terrestrial and satellite communications bandwidth trunks in support of JWICS, SIPRNET, NIPRNET, and similar DoD WAN and MAN architectures. The terms shall also represent low-speed modem bandwidths, e.g., 9.6Kbps terrestrial modem, and radio line of sight (LOS) bandwidth connections from remote stationary or portable sites to a JWICS, SIPRNET, or NIPRNET node.	4.0	Sol/HP/NT	DoDIIS-N-45 16 May 1997
3.2.4.12.18	The default low bandwidth n shall be set to 90 percent for external communications.	4.0	Sol/HP/NT	DoDIIS-N-46 16 May 1997
3.2.4.12.19	The COE shall send a notification to user(s) who have been preempted for low available external communications bandwidth. The notification will be sent n minutes before the user(s) applications are closed and they are logged off.	4.0	Sol/HP/NT	DoDIIS-N-47 16 May 1997
3.2.4.12.20	The default user notification n shall be 5 minutes when about to be preempted for low availability of external communications bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-48 16 May 1997
3.2.4.12.21	The COE CAS shall send a final 45 second notification to user(s) who will be logged off due to low available external communications bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-49 16 May 1997
3.2.4.12.22	The COE CAS shall logoff low priority user(s) due to low available external communications bandwidth.	4.0	Sol/HP/NT	DoDIIS-N-50 16 May 1997
3.2.4.12.23	The COE shall send notification to system administrator(s) when average used external communications bandwidth reaches n percent of available bandwidth	4.0	Sol/HP/NT	DoDIIS-N-51 16 May 1997
3.2.4.12.24	The default average used external communications bandwidth shall be 85 percent.	4.0	Sol/HP/NT	DoDIIS-N-52 16 May 1997
	End			

Table 3.2.4.12: Capacity/Bandwidth Management System Requirements.

3.2.5 Security for Management Operations.

Security NM requirements deal with protecting the NM functionality. Besides general NM security requirements one must also be concerned with security devices that will exist on the network. The security devices can be considered to consist of two main parts: a communications part and a management part. The communications part provides a set of security services to the community of interest on the network. The management part is how the security devices are controlled across the network. A key facet of protecting NM applications is the protocols that are used to manage the devices, systems, and services. Wherever possible these protocols must

operate through a secure means. Equally important is ensuring that alarms are not disabled or tampered with thus preventing the network administrator from knowing the management domain is under attack. Finally, the network administrator must have the necessary tools at their disposal to determine if a network intrusion is occurring and the means by which to terminate the attack.

NM security requirements also include functionality for key management across the network, dial-in terminal server access control, and security NM auditing capabilities. The centralized control of these functions may be implemented either in a security management center on one hardware platform, or in distributed security management centers, each covering a specific management function. This is left up to the chief engineer of a community of interest on how they want to utilize the capabilities.

3.2.5.1 General Security Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.1.1	The different security management functional areas shall be logically separated functions.	3.1+	Sol/HP/NT	NETTWG970522-95 NM.SEC.000
3.2.5.1.2	Security management systems shall allow for remote, on-line management of the security devices and applications.	3.1+	Sol/HP/NT	NETTWG970522-96 NM.SEC.000
3.2.5.1.3	Security management systems shall be kept functionally and logically separate from the network management system(s) of the underlying data network.	3.1+	Sol/HP/NT	NETTWG970522-97 NM.SEC.000
3.2.5.1.4	Security devices which are allowed to communicate shall operate under a common security policy. The security devices may, however, be controlled from different management centers and, hence, belong to different management domains.	3.1+	Sol/HP/NT	NETTWG970522-98 NM.SEC.000
3.2.5.1.5	To the extent possible, the NM system Security Management (SM) capabilities shall be in accordance with the GNMP.	3.1+	Sol/HP/NT	NETTWG970522-99 NM.SEC.000
3.2.5.1.6	If the NM system contains secured IPS-based management components, the minimally acceptable SM requirement is for SNMPv1 management capabilities plus link encryption.	3.1+	Sol/HP/NT	NETTWG970522-100 NM.SEC.000
3.2.5.1.7	The NM system shall support the exchange of, access to, and ability to create, modify, and/or delete management information and parameters associated with security mechanisms, including access control mechanisms, data integrity mechanisms, data origin authentication mechanisms, traffic padding mechanisms, routing control mechanisms, and key generation/distribution mechanisms.	3.1+	Sol/HP/NT	NETTWG970522-139 NM.SEC.000
3.2.5.1.8	The NM system shall support access control list information which includes access-control-oriented managed objects and attributes.	3.1+	Sol/HP/NT	NETTWG970522-141 NM.SEC.000

3.2.5.1.9	The NM system shall access-control-oriented managed objects and attributes that are associated with resource/service-oriented managed objects for the purpose of granting or denying access to the resource/service-oriented managed objects according to the access control policy represented by the access control management information within the access-control-oriented managed objects and attributes.	3.1+	Sol/HP/NT	NETTWG970522-142 NM.SEC.000
3.2.5.1.10	The NM system shall report and archive security-related information such as the reports of individual occurrences of security alarms from specific resources/services.	3.1+	Sol/HP/NT	NETTWG970522-143 NM.SEC.000
3.2.5.1.11	The NM system shall report and archive security-related information such as the archives/audit trails of occurrences of security alarms from specific instances of resources/services, including the conditions of surrounding and associated resources/services, as well as the sequence of effective (and ineffective) corrective actions taken.	3.1+	Sol/HP/NT	NETTWG970522-144 NM.SEC.000
3.2.5.1.12	The NM system shall report and archive security-related information such as the archives of results of all confidence and diagnostic tests pertinent to security testing and/or verification.	3.1+	Sol/HP/NT	NETTWG970522-145 NM.SEC.000
3.2.5.1.13	The NM system shall report and archive security-related information such as the reports of information about when an individual resource/service will resume normal operation if its operation has been effected by a detected or attempted security breach and/or any subsequent corrective actions.	3.1+	Sol/HP/NT	NETTWG970522-146 NM.SEC.000
3.2.5.1.14	The NM system shall report and archive security-related information such as the accounting credit/rebate information pertinent to reduced levels of services that may have arisen subsequent to actual or presumed security attacks recognized by the NM system.	3.1+	Sol/HP/NT	NETTWG970522-147 NM.SEC.000
3.2.5.1.15	The NM system shall be able to send security-related information, as specified or selected by the network security administrator, to network-security-administrator-specified or selected destinations (e.g., a network security administrator's display/monitoring screen, a local information store, an end user of a specific individual resource/service or of a specific class of resources/services, a remote management information data base, etc.).	3.1+	Sol/HP/NT	NETTWG970522-150 NM.SEC.000
	End			

Table 3.2.5.1: General Security Requirements.

3.2.5.2 Device Security Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.2.1	NM shall support user access control for management of network devices.	4.0	NT	Health Affairs NM 11 16 May 1997

	End			

Table 3.2.5.2: Device Security Requirements.

3.2.5.3 Protocol Security Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.3.1	No requirements exist for this section at this time			
	End			

Table 3.2.5.3: Protocol Security Requirements.

3.2.5.4 Alarm Security Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.4.1	The NM system shall support management information to include, threshold levels at which security alarms are triggered, route monitoring and control information, and access control list information.	3.1+	Sol/HP/NT	NETTWG970522-140 NM.SEC.000
3.2.5.4.2	The NM system shall be capable of providing rules-based processing against alarm streams and escalate/de-escalate priorities accordingly.	3.1+	Sol/HP/NT	NETTWG970522-148 NM.SEC.000
3.2.5.4.3	The NM system shall be able to escalate the alarms automatically based on severity and time of opening.	3.1+	Sol/HP/NT	NETTWG970522-149 NM.SEC.000
3.2.5.4.4	The NM system shall support an alarm presentation capability where alarms shall be posted in a graphic oriented alarm pane which corresponds to ISO OSI NMF defined alarm severity and color mapping.	3.1+	Sol/HP/NT	NETTWG970522-152 NM.SEC.000
	End			

Table 3.2.5.4: Alarm Security Requirements.

3.2.5.5 Network Intrusion Security Requirements.

The network intrusion security requirements are subdivided to additional sections to make it easier to track the requirements. The subsections are: detection requirements, analysis requirements, corrective action requirements, recovery requirements, and report security requirements.

3.2.5.5.1 Detection Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.5.1.1	The NM system shall be able to check the possibility of a security attack on managed resources.	3.1+	Sol/HP/NT	NETTWG970522-101a NM.SEC.000
3.2.5.5.1.2	IRT security breach detection, the resource monitoring capabilities shall be used in conjunction with all NM components and system resources to schedule and to execute the monitoring of resources for security breach indications.	3.1+	Sol/HP/NT	NETTWG970522-102 NM.SEC.000
3.2.5.5.1.3	IRT security breach detection, the security alarm report notifications shall be incorporated into management information associated with all NM components and system resources.	3.1+	Sol/HP/NT	NETTWG970522-103 NM.SEC.000
3.2.5.5.1.4	IRT security breach detection, the monitored management information and event reports shall be logged using logging services, log scheduling criteria, log filtering criteria, and log scheduling/filtering control services.	3.1+	Sol/HP/NT	NETTWG970522-104 NM.SEC.000
	End			

Table 3.2.5.5.1: Detection Requirements.

3.2.5.5.2 Analysis Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.5.2.1	The NM system shall be able to diagnose the actual or attempted security violation that was perpetrated on managed resources.	3.1+	Sol/HP/NT	NETTWG970522-101b NM.SEC.000
3.2.5.5.2.2	The NM system shall be capable of analyzing security breach indications using techniques as well as statistical analysis tools to determine root causes of security breach indications.	3.1+	Sol/HP/NT	NETTWG970522-105 NM.SEC.000
3.2.5.5.2.3	The statistical inference and hypothesis testing accuracy measures (i.e., the false positive rates and false negative rates associated with these root cause determinations) used by the NM system security breach techniques shall be greater than 90% correct.	3.1+	Sol/HP/NT	NETTWG970522-106 NM.SEC.000
3.2.5.5.2.4	The NM system security breach analysis capabilities shall include the ability to identify redundant and/or correlated security breach indications.	3.1+	Sol/HP/NT	NETTWG970522-107 NM.SEC.000
3.2.5.5.2.5	The NM system security breach analysis capabilities shall include the ability to assess fault indications and/or to correlate fault indications and security breach indications to identify redundant and/or related phenomena.	3.1+	Sol/HP/NT	NETTWG970522-108 NM.SEC.000

3.2.5.5.2.6	The NM system security breach analysis capabilities shall include the ability to use alarm correlation tools to estimate most likely root causes of suspected security breaches.	3.1+	Sol/HP/NT	NETTWG970522-109 NM.SEC.000
3.2.5.5.2.7	The NM system security breach analysis capabilities shall include the ability to identify the existence of security breaches during conditions when conflicting security breach indications or observations about the state of resources exist.	3.1+	Sol/HP/NT	NETTWG970522-110 NM.SEC.000
3.2.5.5.2.8	The NM system security breach analysis capabilities shall include the ability to verify the existence of security breaches using on-demand, direct inquiries, and tests, of suspicious components, resources, and services, as well as the neighboring components, resources, and services to those suspicious elements.	3.1+	Sol/HP/NT	NETTWG970522-111 NM.SEC.000
3.2.5.5.2.9	The NM system security breach analysis verification capabilities shall include the ability to inject and to monitor test signals and/or test messages at local and remote locations.	3.1+	Sol/HP/NT	NETTWG970522-112 NM.SEC.000
3.2.5.5.2.10	The NM system security breach analysis capabilities shall include the ability to characterize identified security breaches in terms of network/security-administrator-specified/selected parameters (e.g., general geographic location of the security breach (to within an administrator-selectable location granularity).	3.1+	Sol/HP/NT	NETTWG970522-113 NM.SEC.000
3.2.5.5.2.11	The NM system security breach analysis capabilities shall include the ability to characterize identified security breaches in terms of the precise logical/physical location of the security breach (to within an administrator-selectable location granularity).	3.1+	Sol/HP/NT	NETTWG970522-114 NM.SEC.000
3.2.5.5.2.12	The NM system security breach analysis capabilities shall include the ability to use pattern analysis techniques to learn of new events and situations to be monitored for security breach conditions, and to modify security breach detection mechanisms to accommodate and to use such new events and situations to detect new and different types of security breaches.	3.1+	Sol/HP/NT	NETTWG970522-115 NM.SEC.000
	End			

Table 3.2.5.5.2: Analysis Requirements.

3.2.5.5.3 Corrective Action Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments

3.2.5.5.3.1	IRT security attack correction initiation decision-making, the NM system shall have automated abilities to analyze security attack determinations continuously and to recommend whether to initiate corrective actions on a determined security attack.	3.1+	Sol/HP/NT	NETTWG970522-116 NM.SEC.000
3.2.5.5.3.2	IRT security attack correction initiation decision-making, the NM system complexity characteristics of decision criteria for initiating security attack correction activities shall include the ability to trigger a decision based on appropriate factors from the security attack correction policy, such as the pre-defined precedence by which concurrent security attacks are addressed.	3.1+	Sol/HP/NT	NETTWG970522-117 NM.SEC.000
3.2.5.5.3.3	IRT security attack correction initiation decision-making, the NM system complexity characteristics of decision criteria for initiating security attack correction activities shall include the ability to trigger a decision based on appropriate factors from the security attack correction policy, such as the pre-defined precedence of corrective actions to be attempted.	3.1+	Sol/HP/NT	NETTWG970522-118 NM.SEC.000
3.2.5.5.3.4	IRT security attack correction initiation decision-making, the NM system complexity characteristics of decision criteria for initiating security attack correction activities shall include the ability to trigger a decision based on appropriate factors from the security attack correction policy, such as the pre-established levels of acceptable security services, capabilities, and assurance that must be achieved within pre-defined time constraints.	3.1+	Sol/HP/NT	NETTWG970522-119 NM.SEC.000
3.2.5.5.3.5	IRT security attack correction initiation decision-making, the NM system complexity characteristics of decision criteria for initiating security attack correction activities shall include the ability to trigger a decision based on appropriate factors from the security attack correction policy, such as the pre-defined conditions under which different security attack correction strategies/activities shall be undertaken.	3.1+	Sol/HP/NT	NETTWG970522-120 NM.SEC.000
3.2.5.5.3.6	IRT security attack correction actions, the NM system shall have the ability to undertake a variety of corrective actions as selected by the network/security administrator.	3.1+	Sol/HP/NT	NETTWG970522-121 NM.SEC.000
3.2.5.5.3.7	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall be consistent with the security attack correction policy established by the network/security administrator.	3.1+	Sol/HP/NT	NETTWG970522-122 NM.SEC.000
3.2.5.5.3.8	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to change, reset and/or reboot attribute values associated with manageable resources/services.	3.1+	Sol/HP/NT	NETTWG970522-123 NM.SEC.000
3.2.5.5.3.9	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to switch to redundant resources/services.	3.1+	Sol/HP/NT	NETTWG970522-124 NM.SEC.000

3.2.5.5.3.10	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to bypass security compromised resources/services by switching to alternative resources/services (these may not be exactly functionally equivalent to, or have the same performance or security services/capabilities characteristics of, the security compromised resource/service).	3.1+	Sol/HP/NT	NETTWG970522-125 NM.SEC.000
3.2.5.5.3.11	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to disable security compromised resources/services.	3.1+	Sol/HP/NT	NETTWG970522-126 NM.SEC.000
3.2.5.5.3.12	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to isolate security compromised resources/services from the operational network by disabling all links attached to it. This prevents the spread of security attacks and/or faults to other resources/services (e.g., as might be the case with attacks caused by roving viruses).	3.1+	Sol/HP/NT	NETTWG970522-127 NM.SEC.000
3.2.5.5.3.13	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to use software distribution to replace compromised and/or virus-infected software in faulty resources.	3.1+	Sol/HP/NT	NETTWG970522-128 NM.SEC.000
3.2.5.5.3.14	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to request manual replacement of compromised resources/services.	3.1+	Sol/HP/NT	NETTWG970522-129 NM.SEC.000
3.2.5.5.3.15	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to request on-line or off-line repair of compromised resources/services.	3.1+	Sol/HP/NT	NETTWG970522-130 NM.SEC.000
3.2.5.5.3.16	IRT security attack correction actions, the corrective actions undertaken and the speed with which they are completed shall include the ability to open trouble/repair ticketing and tracking activities on the compromised resource/service and associated work order tickets.	3.1+	Sol/HP/NT	NETTWG970522-131 NM.SEC.000
3.2.5.5.3.17	IRT security attack correction tracking, the NM system shall have the ability to track the status of on-line correction actions as well as off-line repair activities.	3.1+	Sol/HP/NT	NETTWG970522-132 NM.SEC.000
3.2.5.5.3.18	IRT security attack correction tracking, the NM system shall have the ability to provide estimates of the expected time to complete initial and/or minimal security restoral.	3.1+	Sol/HP/NT	NETTWG970522-133 NM.SEC.000
3.2.5.5.3.19	IRT security attack correction tracking, the NM system shall have the ability to provide estimates of the expected time to return to full survivability levels and security levels.	3.1+	Sol/HP/NT	NETTWG970522-134 NM.SEC.000
3.2.5.5.3.20	The NM system shall have the ability to verify security attack correction through on-demand, network/security-administrator-selectable testing.	3.1+	Sol/HP/NT	NETTWG970522-135 NM.SEC.000

	End			

Table 3.2.5.5.3: Corrective Action Requirements.

3.2.5.5.4 Recovery Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.5.4.1	The NM system security attack network/security-administrator-selectable testing shall be able to assure that a given resource or service is ready to be restored with requisite security characteristics and that repair/replace activities have been successfully completed.	3.1+	Sol/HP/NT	NETTWG970522-136 NM.SEC.000
3.2.5.5.4.2	As appropriate, the NM system automatically shall close associated trouble tickets upon successful verification that a security attack related compromised resources/service has been restored.	3.1+	Sol/HP/NT	NETTWG970522-137 NM.SEC.000
	End			

Table 3.2.5.5.4: Recovery Requirements.

3.2.5.6 Reports Security Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.5.6.1	No requirements exist for this section at this time			
	End			

Table 3.2.5.6: Reports Security Requirements.

3.2.6 Coexistence of OSI-Based and IPS-Based NM Technologies.

It is common knowledge that certain segments of the marketplace are currently dominated by legacy or proprietary management standards, or management capabilities. Some of these are based on the Internet Protocol Suite standards while others are not. Furthermore, it is widely accepted that these legacy systems will have to coexist with newly-acquired systems built upon open, voluntary standards such as IPS and Open Systems Interconnection. Previously fielded management components and capabilities do not need to be replaced as long as they are

operationally and economically viable. However, as the legacy management capabilities are upgraded or replaced they will need to be based on a fully integrated and fully interoperable, open management system capability. DOD can no longer support proprietary management components in lieu of open systems standards. The upgraded legacy system or new management system will run on the DII COE in keeping with the JTA directive. Being DII COE-compliant will go a long way toward improving interoperability between systems.

All newly-acquired IPS-based resources in the DOD are to be manageable by DOD personnel by use of both IPS-based and OSI-based management systems. All newly-acquired OSI-based resources in the DOD are to be manageable by the use of OSI-based management systems. The intent here is not to require native OSI managed objects within IPS-based resources. Rather, the intent is, in an enterprise management environment, to make the management of IPS-based resources visible to OSI-based management by appropriate management gateways.

The following are DII COE NM requirements for the coexistence of OSI-Based and IPS-Based NM technologies.

3.2.6.1 General Coexistence Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.6.1.1	NM shall support management of networking entities from different vendors, both SNMP and non-SNMP, including hubs, routers, software servers, file-servers, telecommunication switches, and computer workstations.	4.0	NT	Health Affairs NM 9 16 May 1997
	End			

Table 3.2.6.1: General Coexistence Requirements.

3.2.6.2 Alarm Coexistence Requirements.

Paragraph Number	Requirement Description	Desired COE Build	Targeted Operating System	Comments
3.2.6.2.1	No requirements exist for this section at this time			
	End			

Table 3.2.6.2: Alarm Coexistence Requirements.

3.3 CSCI External Interface Requirements.

3.3.1 Interface Identification and Diagrams.

None.

3.3.2 Project-Unique Identifier of Interface.

3.3.2.1 Software Interfaces.

The NM functional area has dependencies on other functional areas of the DII COE. These areas include, but are not limited to, the following:

Office Automation
Online Help
Data Access Services
Alerts
Message Processing
Presentation Services
Web Server
Communications
Message Processing
Global Data Management Services
Data Management Services
Distributed Computing Services
Operating System Services

3.3.2.1.1 The NM functional area applications shall provide standard Applications Programmer's Interfaces (APIs) to allow other non-network applications to access Network Management application functionality where possible. The viability of APIs in COTS and GOTS will vary widely. DISA will strive to have 100% exposure of APIs in GOTS applications and best case in COTS applications.

3.3.2.1.2 The NM functional area software shall support services provided by COTS products which operate with the Operating System (i.e., DCE, Informix, CORBA, etc.).

3.3.2.2 Input/Output Devices.

3.3.2.2.1 The NM functional area shall support the RS232 interface to external systems.

3.3.2.2.2 The NM functional area shall support external SCSI devices used for communications devices or other communications uses.

3.3.2.2.3 The NM functional area shall support Ethernet interfaces for local area networks.

3.3.2.2.4 The NM functional area shall support peripheral devices used for printing functions.

3.3.2.2.5 The NM functional area shall support peripheral devices used for plotting functions.

3.3.2.3 Input/Output Interfaces.

3.3.2.3.1 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces to asynchronous serial I/O devices in the form of operating system device drivers and supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.2 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces to synchronous serial I/O devices in the form of operating system device drivers and supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.3 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces using Transmission Control Protocol (TCP)/ Internetwork Protocol (IP) in the form of operating system device drivers and supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.4 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces using UDP in the form of operating system device drivers and supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.5 The NM functional area shall provide the Telnet Upper Layer protocol (OSI Layer 7) and services. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.6 The NM functional area shall provide the File Transfer Protocol (FTP) Upper Layer protocol (OSI Layer 7) and services. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.7 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces using Serial Line Interface Protocol (SLIP) in the form of operating system device drivers and supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.8 The NM functional area shall provide the Transport (OSI Layer 4) and Lower Layer interfaces using Point to Point Protocol (PPP) in the form of operating system device drivers and

supporting processes. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.9 The NM functional area shall provide the Ping Upper Layer protocol (OSI Layer 7) and services. This protocol is usually supplied with the POSIX compliant Operating System or may be added as COTS.

3.3.2.3.10 The NM functional area shall support the interface to the NIPRNET, SIPRNET, and JWICS IP networks (or to unclassified, secret, top secret, and SCI secure level data networks).

3.3.2.4 Interface Definition.

3.3.2.4.1 The interface definition, Application Programming Interface (API), for the NM function area applications to be accessed by the Application or Higher Layer software shall be identified and described in the Application Programming Interface Reference Manual (APIRM) identified in the DDR.

3.3.2.4.2 The NM functional area software APIs for interfacing to Transport, Network and Data Link Layer services shall be described in accordance with standard or well accepted defacto industry interfaces.

3.3.2.4.3 The NM functional area software shall support the interface definition provided by COTS products (TCP/UDP, IP, PPP, etc.). Network Services shall define a set of standards and mechanisms for the construction of network management interfaces.

3.3.2.4.4 The NM functional area software shall support the interface definition provided by COTS products (TCP/UDP, IP, PPP, etc.). Network Services shall define a set of standards and mechanisms for the construction of network management interfaces.

3.4 CSCI Internal Interface Requirements.

The design of the network management internal interfaces has not been determined at this time. If necessary, these requirements will be developed during the software design process.

3.5 CSCI Internal Data Requirements.

Internal data requirements have been included in the requirements identified in Section 3.2.

3.6 Adaptation Requirements.

None.

3.7 Safety Requirements.

Safety is the responsibility of the overall system into which the segmented network management applications software is embedded. The network management software shall not interfere with, nor defeat the purpose of, safety functions implemented in the host system.

3.8 Security and Privacy Requirements.

The network management functional area provides for the management of a network in association with the systems management applications and security management applications. It shall consist of a set of network management applications entities and a management communications protocol stack.

The network management functional capabilities shall be accreditable initially for the system high mode of operation. This is for both a distributed network environment and for a standalone environment.

The network management functions shall be logically separated from other management functions, such that only authorized users can access them.

The network management security constraints and devices shall operate under a common security policy. The security devices may, however, be controlled from different management centers and hence belong to different management domains.

3.9 CSCI Environment Requirements.

The NM functional area shall execute on all hardware and software platforms supported by the DII COE program under the cognizant control of the DII COE Engineering Office as specified within the bounds of Section 3.2.

3.10 Computer Resource Requirements.

3.10.1 Computer Hardware Requirements.

As described earlier, the DII COE is a foundation for a designer to build systems on. It is not a system by itself though each component of the DII COE (kernel, infrastructure support applications, and common support applications) does require a certain amount of hard disk space and RAM to operate with. The designer of a DII COE-compliant system must determine the combined hardware requirements of the operating system, the DII COE kernel, the DII COE infrastructure services and the DII COE common support applications segments, and their mission

application segments which will be loaded onto a hardware platform. Only after a thorough examination of each of these software components can the hardware be properly sized.

3.10.2 Computer Hardware Resource Utilization Requirements.

The DII COE kernel installation procedures identify how much hard disk space and RAM is required to run that version of the DII COE kernel for a specific operating system. These specifications, in conjunction with operating system specifications, should be used as the minimum essential starting point for the designer of a DII COE-compliant system.

3.10.3 Computer Software Requirements.

The DII COE kernel installation procedures identify the size of the kernel software in megabytes. Only the DII COE kernel is required on a workstation in order for the workstation to be considered DII COE-compliant. It is the responsibility of the designer of a DII COE-compliant system to decide which additional DII COE infrastructure services and common support applications segments will be loaded beside the mission applications. The DII COE-compliant network management applications are considered part of the infrastructure services layer of the DII COE.

3.10.4 Computer Communications Requirements.

Communications requirements are associated with end system designs. Since the DII COE is a foundation, this section does not apply. The designer of a DII COE-compliant system must determine these characteristics for their system based on operational needs of the community of interest.

3.11 Software Quality Factors.

Software quality factors are applied differently to NM applications based on their source, GOTS or COTS. The design of any GOTS network management applications software will be in line with the software quality factors identified in the software developer's contract or derived from a higher level specification. It is much more difficult for DOD programs to influence the quality of commercially designed software than it is GOTS so it's difficult to hold COTS software to a particular set of standards. However, for COTS applications, software quality factors may be used as decision criteria for choosing one product over another for inclusion in the DII COE when there are two or more applications of equivalent functionality. Examples of software quality factors include reliability, maintainability, availability, flexibility, portability, reusability, testability and usability (the ability to be easily learned and used). Another factor to consider is the source of COTS is a manufacturer or a reseller and what technical support agreements exist for maintaining the products.

3.12 Design and Implementation Constraints.

3.12.1 Dependencies on Other Software.

Many of the network management applications require a supporting Relational Data Base Management System (RDBMS) to maintain the application specific data. The RDBMSs currently supported by the DII COE Engineering Office are:

DII COE Version 3.1	Oracle 7.3.2.3	Solaris 2.5.1 and HP-UX 10.20
	Sybase 10.2.2.4	Solaris 2.5.1 and HP-UX 10.20
	Informix 7.12	Solaris 2.5.1
	Informix 7.22	Solaris 2.5.1 and HP-UX 10.20
	MS Access	NT 4.00

3.12.2 Supported Operating Systems.

Segmented network management applications may support any or all of the following operating systems based on the documented requirements. Section 3.2 identifies which requirements are required against a particular DII COE supported operating system. Those operating systems that are currently supported by the DII COE Engineering Office are:

DII COE Version 3.1	Solaris 2.5.1
	HP-UX 10.20
	NT 4.00

3.12.3 Client/Server Environment.

Segmented network management applications must operate in a distributed client/server computing environment. This does not preclude client and server applications from being loaded onto the same workstation.

3.13 Personnel-Related Requirements.

Not applicable. Personnel-related requirements must be determined by the developers of the DII COE-compliant system in which the network management applications are embedded. It is strongly recommended that a DII COE-compliant system have a network administrator function but the size and scope of this position is outside the purpose of this document.

3.14 Training-Related Requirements.

Not applicable. Training requirements must be determined by the developers of the DII COE-compliant system in which the network management applications are embedded. In almost all cases the network management requirements will be satisfied by COTS network management applications. The developers of the DII COE-compliant systems may choose to use commercial training since most vendors do offer classroom instruction on their applications. In some cases there may be a military school that covers the network management applications in question.

3.15 Logistics-Related Requirements.

The Network Management function area has no unique logistics requirements in that the DII COE is a foundation and not a system. Any DII COE-compliant system must meet the logistics requirements as called out in the appropriate logistics plan for that community of interest.

3.16 Other Requirements.

All segmented network management applications for use in a DII COE-compliant system will be IAW the DII COE I&RTS. Applications must achieve a Level 5 compliance or higher before they are considered fieldable.

3.17 Packaging Requirements.

Network management applications segments will be formatted in accordance with the I&RTS. This requires that the segments can be read and installed by the COEInstaller tool distributed as part of the DII COE kernel. This does not imply that a specific network management application, in segmented form, will be available for ***all*** supported operating systems of the DII COE. The DII COE Engineering Office only gives direction to developers to produce segmented products for use on the various operating systems for which there is a documented requirement.

The DISA OSF Configuration Management Department is the central distribution facility for DII COE segments. Segments are distributed to DISA-sponsored programs, DII COE Engineering Office developers, and to S/A distribution centers (e.g., AF, Army, DoDISS, etc.). S/A users and developers with S/A distribution centers must go through their cognizant DII COE distribution POC and not the DISA OSF facility. Please consult the DII COE HomePage for up-to-date information on software availability and distribution.

3.18 Precedence and Criticality of Requirements.

The order of precedence of the main areas identified in Section 3.2 indicating the relative importance of the requirements in this document is as follows:

- Coexistence of OSI-Based and IPS-Based NM Technologies.
- Management Architecture.
- Management System Characteristics.
- Management Components.
- Management Applications.
- Security for Management Operations.

The above specifies the general order of precedence of the main areas identified in Section 3.2. Specific order of precedence or criticality for individual requirements is identified and prioritized in Section 5, Requirements Traceability.

4. Qualification Provisions.

This section defines the qualification methods used to ensure that the functional requirements identified in Section 3.2 have been met. However, these functional requirements only identify how DII COE-compliant network management applications must behave. They do not address the level of compliance of the network management application segments in accordance with the DII COE I&RTS. Segments must be at least Level 5 compliant before they can be considered fieldable. It would not be appropriate for segmented network management applications to be compared against Section 3.2 if the segments fail to obtain Level 5 compliance.

Those network management applications that are considered an integral part of the DII COE and fall under the direct control and supervision of the DII COE Engineering Office (DISA/JEXF-OSF) are delivered to the DISA OSF for testing. Developers of these DII COE segmented applications are required to deliver documentation in accordance with the *Configuration Management Software and Documentation Delivery Requirements (DDR)* document. The DDR references a second document, the *Defense Information Infrastructure (DII) Common Operating Environment (COE) Developer Documentation Requirements*. Both the DDR and the DDDR documents specify a number of documents that all DII COE developers must submit unless the DII COE Engineering Office has granted waivers. Three of the required documents are the Software Test Plan (STP), the Software Test Description (STD), and the Software Test Report (STR). The STP document describes the types of tests required and provides traceability to the software requirements the segments satisfy. The STP identifies the test locations, describes the test environment, and provides details concerning resources required for testing. The STD document describes the test cases and acceptance criteria that will be used to test the software. It describes the test methods, tools, scenarios, and the pass/fail criteria for assessing the results of the testing. The STD shall provide all essential information relating to each test so that an independent test can duplicate the test results or verify the results obtained. The final document in the trio is the STR. The STR document provides a technical report with supporting documentation (package of materials) required to evaluate the results of the software tests described in the STD. The STR documents the results of all tests run against the software, identifies problems encountered during testing, and recommends solution to those problems. These three documents are crucial in determining which requirements the segments satisfy.

The segmented network management applications will be qualified through formal validation tests in comparison to the SRS Section 3.2 requirements. The Qualification Methods applied to the segmented software shall include Compliance Test (CT), Test (T), Demonstration (D), Analysis (A), and Inspection (I).

Compliance Test (CT): A qualification method that is carried out by testers at the DISA OSF for DII COE applications. Applications segments are examined using the eight levels of compliance identified in the I&RTS. Test data is collected and subsequently examined to determine the actual level of compliance for each segment tested IAW the DII COE I&RTS. The data and tester's

recommendations of a pass/fail, based on Level 5 compliance, are formulated into a test report and sent to the DII COE Engineering Office for final evaluation.

Test (T): A qualification method that is carried out by operation of the item, component, interface, or some part of the computer software configuration item that relies on the collection and subsequent examination of data. The collection of the data can be done using instrumentation or other specialized test equipment. In most cases this type of testing refers to functional testing. In the case of GOTS network management software, functional testing is performed at the location designated by the DII COE Engineering Office. This testing encompasses the full breadth and scope of the GOTS application and ensures it meets the design criteria. Functional testing of COTS software is treated differently. The only functional testing performed at the DISA OSF is to ensure the segmented application launches, runs, and closes gracefully. Functional testing of the commercially baselined product is left up to its global customer base.

Demonstration (D): A qualification method that is carried out by operation of the item, component, interface, or some part of the computer software configuration item that relies on observable functional operation not requiring the use of elaborate instrumentation or special test equipment. Typically, this qualification method is one of the easiest to perform.

Analysis (A): A qualification method that is carried out by the processing of accumulated data. An example of accumulated data is the compilation of data obtained from other qualification methods. The processing of the accumulated data normally involves interpretations or extrapolations made from the test data results. After the reduction, interpretation, or extrapolation of test data results a decision can then be made of whether the requirement in question has been satisfied.

Inspection (I): A qualification method that is carried out by visual examination, physical manipulation, or measurement to verify that the requirements have been satisfied. This may involve the visual examination of code, documentation, etc.

Special qualification methods may also be applied to the item, component, interface, or some part of the computer software configuration item that require special tools, techniques, procedures, facilities, and acceptance limits beyond those identified above.

5. Requirements Traceability.

This section in its entirety will be removed from the document prior to posting on the DII COE HomePage or any other web site. Please reference the distribution statements on the cover page of this document for further guidance.

5.1 Objectives of Traceability.

Traceability, in the context of the DII COE, means that each of the requirements identified in section 3.2, *Network Management (NM) Functional Area Capability Requirements*, of this document is associated with a segment or collection of segments that satisfies the requirement. The segments that satisfy the requirement may differ by the DII COE Version, the supported operating system, or both. The matrixes in section 5.2 will identify this level of detail.

5.2 Requirements Matrixes.

At this time there are no DII COE-compliant NM applications available on the DII COE. Several applications are scheduled for initial delivery during the summer of 1997. Once segmented NM applications are available, this section will be completed.

6. Notes.

6.1 Acronyms.

The acronyms used in this document are defined as follows:

A	-	Analysis
AIS	-	Automated Information Systems
AM	-	Accounting Management
ANSI	-	American National Standards Institute
AOG	-	Architectural Oversight Group
API	-	Application Programming Interface
APIRM	-	Application Programming Interface Reference Manual
C2	-	Command and Control
C4I	-	Command, Control, Communications, Computers, and Intelligence
CCITT	-	International Telegraph and Telephone Consultive Committee
CFCSE	-	Center for Computer Systems Engineering
CJCSI	-	Chairman, Joint Chief of Staff Instruction
CJCSM	-	Chairman, Joint Chief of Staff Manual
CM	-	Configuration Management
CMIP	-	Common Management Information Protocol
CMIS	-	Common Management Information Services
COE	-	Common Operating Environment
COMSEC	-	Communications Security
CONOPS	-	Concept of Operations
CONUS	-	Continental United States
COTS	-	Commercial Off-the-Shelf
CS	-	Communications Servers
CSCI	-	Computer Software Configuration Item
CT	-	Compliance Test
CTO	-	Cognizant Technical Official
D	-	Demonstration
DAA	-	Designated Accreditation Authority
DBMS	-	Database Management System
DCE	-	Distributed Communication Environment
DCS-EP	-	Defense Communications System Entry Point
DDN	-	Defense Data Network
DDR	-	Developer Documentation Requirements
DDDR	-	DII COE Developer Documentation Requirements
DDRS	-	Defense Data Repository System
DES	-	Data Encryption Standard
DID	-	Data Item Description

DII	-	Defense Information Infrastructure
DIICC	-	Defense Information Infrastructure Control Concept
DISA	-	Defense Information Systems Agency
DISN	-	Defense Information Systems Network
DME	-	Distributed Management Environment
DMS	-	Defense Message System
DOD	-	Department of Defense
DODIIS	-	DOD Intelligence Information Systems
DODISS	-	DOD Index of Specifications and Standards
DSCS	-	Defense Satellite Communications System
DSN	-	Defense Switched Network
EA	-	Executive Agent
E-mail	-	Electronic mail
FDDI	-	Fiber Distributed Data Interface
FIPS	-	Federal Information Processing Standard
FM	-	Fault Management
FTP	-	File Transfer Protocol
FY	-	Fiscal Year
GCC	-	Global Control Center
GCCS	-	Global Command and Control System
GCSS	-	Global Combat Support System
GDMO	-	Guidelines for the Definition of Managed Objects
GFE	-	Government Furnished Equipment
GFI	-	Government Furnished Information
GMC	-	GCCS Management Center
GNMP	-	Government Network Management Profile
GOSIP	-	Government Open Systems Interconnection Profile
GOTS	-	Government Off-the-Shelf
GUI	-	Graphical User Interface
I	-	Inspection
I&RTS	-	Integration and Runtime Specification
IAB	-	Internet Architecture Board
IAW	-	In accordance with
IEC	-	International Electrotechnical Committee
IEEE	-	Institute of Electrical and Electronics Engineers
IGOSS	-	Industry/Government Open Systems Specification
IOC	-	Initial Operational Capability
IP	-	Internet Protocol
IPS	-	Internet Protocol Suite
IRT	-	In reference to
ISO	-	International Organization for Standardization
ITSDN	-	Integrated Tactical Strategic Data Networking

ITU-TS	-	International Telecommunication Union - Technology Sector
JDIICC-D	-	Joint Defense Information Infrastructure Control Center - Deployed
JIEO	-	Joint Interoperability and Engineering Organization
JTF	-	Joint Task Force
JTA	-	Joint Technical Architecture
JWICS	-	Joint Worldwide Intelligence Communications System
LAN	-	Local Area Network
LCC	-	Local Control Center
LLC	-	Logical Link Control Protocol
MAN	-	Metropolitan Area Network
MFA	-	Management Functional Area
MIB	-	Management Information Base
MIB-II	-	the current implementation of the Internet MIB
MIL-STD	-	Military Standard
MLS	-	Multi-Level Security
MTBF	-	Mean Time Between Failure
MTTF	-	Mean Time To Failure
MTTR	-	Mean Time To Repair
NATO	-	North Atlantic Treaty Organization
NCA	-	National Command Authority
NCC	-	Network Control Center
NE	-	Network Element
NETTWG	-	Network Management Services Technical Working Group
NIPRNET	-	Unclassified Internet Protocol Router Network
NIST	-	National Institute of Standards and Technology
NLSP	-	Network Layer Security Protocol
NM	-	Network Management
NMCC	-	National Military Command Center
NMF	-	Network Management Forum
NTIS	-	National Technical Information Services
OIW	-	OSE Implementors' Workshop
OPR	-	Office of Primary Responsibility
OSD	-	Office of the Secretary of Defense
OSE	-	Open Systems Environment
OSF	-	Open Software Foundation
OSF	-	Operational Support Facility
OSI	-	Open Systems Interconnection
PDU	-	Protocol Data Unit
PM	-	Performance Management
PPP	-	Point-to-Point Protocol
PSAP	-	Presentation Service Access Point
RCC	-	Regional Control Centers

RDBMS	-	Relational DBMS
RDA	-	Remote Database Access
RFC	-	Request for Comment (IETF)
RPC	-	Remote Procedure Call
RMON	-	Remote Monitoring
ROSE	-	Remote Operations Service Element
S/A	-	Service/Agency
SCI	-	Sensitive Compartmented Information
SDNS	-	Secure Data Network Systems
SECRET-NOFORN	-	Secret-Not Releasable to Foreign Nationals
SIPRNET	-	Secret Internet Protocol Router Network
SLIP	-	Serial Line Interface Protocol
SM	-	Security Management
SMFA	-	Specific Management Functional Area
SMI	-	Structure of Management Information
SMP	-	Simple Management Protocol
SNMP	-	Simple Network Management Protocol
SNMPv1	-	Simple Network Management Protocol, Version 1
SNMPv2	-	Simple Network Management Protocol, Version 2
SP4	-	SDNS Security Protocol at Layer 4
SPIRIT	-	Service Provider Integrated Requirements for Information Technology
SQL	-	Structured Query Language
SRS	-	Software Requirements Specification
STD	-	Software Test Description
STP	-	Software Test Plan
STR	-	Software Test Report
T	-	Test
TAFIM	-	Technical Architecture Framework for Information Management
TCP	-	Transmission Control Protocol
TCP/IP	-	Transmission Control Protocol/Internet Protocol
TBD	-	To Be Determined
TDY	-	Temporary Duty
TLSP		Transport Layer Security Protocol
TOP	-	Technical and Office Protocol
TP	-	Transaction Processing Protocol
UDP	-	User Datagram Protocol
VT	-	Virtual Terminal
WAN	-	Wide Area Network
XMP	-	X/Open Management Protocol

6.2 List of Terms and Definitions.

The following definitions and explanatory information are applicable for the purpose of this document.

Accounting Management (AM). AM is one of the five major Management Functional Areas (MFAs) that is described in the ISO OSI Management Framework and System Management Overview standards. The AM MFA defines requirements to enable identification or negotiation of mechanisms for associating and collecting system resource usage charges, to initiate or deactivate charging algorithms, and to monitor or to report account relevant information.

Attribute. An attribute is a property of a managed object and has a value. Mandatory initial values for attributes can be specified as part of the managed object class definition. Attributes are grouped into mandatory and conditional packages.

Common Management Information Services and Common Management Information Protocol (CMIS/CMIP). CMIS and CMIP are the services and protocol developed by ISO for OSI systems management. CMIP is the protocol used by an application process to exchange information and commands for the purpose of remotely managing computer and communication resources, while CMIS specifies the service interface to CMIP. CMIS/CMIP may be used over a variety of underlying protocol stacks, including full-stack OSI, a mixed upper layer OSI over TCP/IP, and just the IEEE lower layer stack (LLC and below). In the former case, in order to transfer management information between open systems using CMIS/CMIP, peer connections (associations) must be established. This transfer requires the establishment of an application association, a session connection, a transport connection, and, depending upon the underlying communications technology, network and link connections.

Configuration Management (CM). CM is one of the five major MFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The CM MFA defines requirements to determine/monitor (via interrogation, polling or event-driven reporting), to detect changes in, and to control the arrangement, relationships, characteristics and state (for example, initialize/terminate, activate/deactivate, idle/busy, etc.) of individual and specifiable aggregates of managed resources so as to maintain continuous operation and/or delivery of service. CM as used in this document is not to be confused with CM as used in MIL-STD-483 (Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs) or MIL-STD-1456 (Configuration *Management Plan*).

Databases. Databases are archival repositories persistently stored on electro/optical media. Databases are accessed or updated by database management systems. Databases are generally used by, and shared among, manager systems by means of standard database query languages, such as SQL and RDA. Some databases may be integrated across several different manager systems and/or management domains.

Directory Services. The Directory Services (IS 9594, CCITT X.500) is an application service which enables users to query on the names of other users (for example, message recipients, applications, host names) and to obtain additional network information (for example, originator/recipient addresses, application entity titles, Presentation Service Access Point (PSAP) of application entities, and network address of host computers).

Domains. Domains represent different ways of aggregating and distributing management authority and/or management scope for any specific reason. Often, large, complex aggregations of resources are partitioned into domains to make the inherent complexity manageable. An illustrative domain partitioning is between telecommunications service providers and their service users. The provider domain consists of the provider-owned physical and logical resources that make up the provider's network. The user domain consists of the user-owned resources that comprise the user's private network. The services obtained from the provider domain may or may not be considered to be in the user's domain, while the resources that underlie these services are definitely not in the user's domain.

Enterprise Management. Enterprise management is the management of the aggregate of all systems and networks within an organization or enterprise.

Event. An event is any occurrence that changes the status of a managed object. The event may be spontaneous or planned, persistent or temporary, and may trigger other events or be triggered by other events.

Fault Management (FM). FM is one of the five major MFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The FM MFA defines requirements to define, detect, identify, monitor, isolate the causes of, log, analyze, test for, trace and correct problems in abnormal or disabled managed resources.

Government Network Management Profile (GNMP). The GNMP is defined in FIPS Publication 179, *Government Network Management Profile (GNMP)*, dated 15 Dec. 92. Section 2 identifies how one can electronically retrieve the document from a government file server.

Hot Backups. Hot backups are fully configured sites which can take over all the functions of the primary site they are backing up. They are set up to come on-line within a short time after the primary site fails or is taken off-line (for example, maintenance).

Human Engineering. Human engineering is the consistent presentation of management information from heterogeneous network resources (for example, help screens, summarized data, graphical user interfaces, ergonomics, etc.). The use of human engineering will enable the network manager to quickly and easily comprehend the NM system's capabilities, to use the NM functions efficiently, and to allow flexibility in performing the desired operations.

Managed Object. Managed objects are abstract representations of resources in a network. A managed object may represent a physical entity, a network service, or an abstraction of a resource which exists independently of its use in management. Managed object definitions of OSI resources, a critical requirement for interoperable NM systems, are beginning to be standardized. IS 10165-4 contains a set of standard guidelines for the definition of managed objects. IS 10165-2 and a number of the International Organization for Standardization/International Electrotechnical Committee (ISO/IEC) 10164 series of standards contain definitions of common management information that can be imported into definitions of managed objects. Due to the importance of managed object definitions, many standards groups, vendors and user consortia (for example, CCITT, the IEEE 802, the NMF and the OIW (Open Systems Environment Implementors Workshop) NM Special Interest Group) are defining managed objects. The DOD has been active in defining military-unique managed objects. Specifically, MIL-STD-2204, SAFENET, defines a number of managed objects which are used to support the synchronization of distributed clocks in a tactical shipboard local area network.

Managed System. Managed systems contain agent processes that act on behalf of, and therefore interact with, remote manager systems or managed resources. The agent processes interact directly with the managed objects that characterize the managed resources. A single object may represent one or many resources, and a single resource may be characterized by one or many objects (each providing different management views of the actual resource). Such managed systems are often embedded in the hardware and/or software of the resource to be managed.

Management Domain. A management domain is a set of managed objects which is accessible from a single management authority. For instance, a key management center may be associated with a key management domain. Within a security domain, however, a key management domain, an access control domain, and an audit management domain must overlap.

Management Gateways. Management gateways translate and map between different management communication protocols, services, and/or different styles of representing the management information associated with specific resources. Such differences typically arise between (a) manager systems, such as n-layer managers or element managers, and (b) manager systems that manage an entire system. Differences also arise between managers of entire, but different, systems, such as managers of different protocol stacks. Management gateways can be used to accommodate management of existing, legacy resources. Management gateways can also be used to accommodate management of other future resources.

Management Information Base (MIB). A MIB is a distributed repository of the management information that represents the resources being managed. MIBs are also runtime, real-time repositories available to be shared among manager systems, managed systems, and management gateways by means of standard management communication protocols. Many types of MIBs exist.

Manager System. A manager system is the hardware and software entity which receives management inputs from local operators, receives management inputs (such as spontaneous management-related notifications) from agent processes in remote manager systems (or in remote managed systems) and/or initiates requests for management information from agents in remote manager systems or in remote managed systems. (Management communications with remote manager systems or managed systems may occur via a standard, general purpose management communications protocol, such as CMIP.) A manager system can make management decisions via supported management applications. A manager system can effect decisions and other management operations either locally on local managed objects or remotely to manager systems or to managed systems representing remote managed objects.

Network. A network is a connected set of switching and transmission communication components. The network includes all hardware and software communications components residing in such switching and transmission components, as well as in end-systems, such as computers, that are attached to the network.

Network Administrator. A network administrator is the person responsible for operating a NM system.

Network Control Center (NCC). A NCC is the top-level DOD NM entity within a management domain. The NCC coordinates and controls NM functions within a domain and between domains.

Network Management (NM). NM is the set of activities to bring up and establish networking resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, the term is also used to refer to such management activities as well as a myriad of other management functions and activities, of greater or lesser scope, when any of such management functions and activities are applied to other kinds of manageable resources besides telecommunications (voice), messaging, video and computer communications networks. Other such management functions and activities may be associated with the early planning stages, growth and retirement of resources, as well as with daily operation and utilization. Other such resources may include general purpose information processing resources such as computers, their system software/peripherals, the distributed multimedia applications they host, or the aggregate of all such resources together with the networking resources used to interconnect them.

Network Management System (NM system). An NM system is the aggregate of the operational and administrative mechanisms, protocols, procedures and tools to provide NM. The NM system may consist of manager systems, managed systems, and management gateways.

Network Manager. A network manager is a specialized manager system used to manage networking resources.

N-layer Manager. An n-layer manager is a manager that manages the resources specific to one layer of a stack of networking protocols. Such managers often do not use general purpose management communication protocols (for example, CMIP), services and management information. Rather, they often use mechanisms and/or services specific to the protocol layer being managed.

Package. A package is a term used in the definition of OSI managed objects. A package refers to a collection of attributes, notifications, operations, and/or behaviors which are treated as a single module in the specification of a managed object class. Packages may be specified as mandatory or conditional when referenced in a managed object class definition. However, the provision of options in managed object class definitions is discouraged on the grounds that internetworking becomes more difficult as the number of conditional packages increases.

Performance Management (PM). PM is one of the five major MFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The PM MFA defines requirements to provide the attributes, services, and event reports to measure, estimate, monitor (via interrogation, polling or event driven reporting), track, store, analyze/evaluate, maintain and otherwise control the configuration, operational characteristics, performance/effectiveness characteristics, performance measuring/monitoring characteristics, performance tuning characteristics, performance testing characteristics and/or quality-of-service characteristics and objectives (for example, responsiveness, availability, utilization, and residual capacity) associated with individual managed resources or specifiable aggregates of managed resources.

Router. A router is a device that provides the network layer relay function connecting two subnetworks. That is, the device receives data from one network entity and forwards it to another network entity.

Security Domain. A security domain is a set of entities that is subject to a single security policy and administered by a single authority. The entities within a particular security domain may be related to a functional or geographic area. A security domain relates to a collection of security devices and their management centers. A particular security device may operate within more than one security domain. In this case, exact rules must exist to regulate which security policy to follow for each instance of communications.

Security Management (SM). SM is one of the five major MFAs that is described in the ISO OSI Management Framework and System Management Overview standards. The SM MFA defines requirements to support combat of threats by identifying and logging users of sensitive resources, monitoring usage of sensitive resources, defining, identifying, and monitoring security-relevant events, creating, and analyzing audit trails of such events, users and usage, controlling certain aspects of security services and mechanisms (for example, initiating re-keying or algorithm

reinitialization), and controlling configurations (for example, isolating infected resources or denying/limiting resource access to unauthorized applications, users, or their requests).

Management Functional Area (MFA). ISO has partitioned systems management into five MFAs to categorize requirements for the support of systems management. The five MFAs are: configuration management, fault management, performance management, security management, and accounting management. System Management Function standards define management services/capabilities to meet these requirements. In some cases, different MFAs have the same requirements and therefore use the same System Management Functions (SMFs) to satisfy the common requirements.

System. A system is a set of information processing and data processing resources (such as computers), together with any supporting system software (such as operating systems and DBMSs), any peripheral devices, any supported applications and files, and any communications infrastructure that interconnects the system's components, end-users of such system resources, and the users and components of other systems. A system is generally considered to include all hardware and software components, facilities, personnel, and procedures which are necessary to support applications.

Systems Management. Systems management is the set of activities to bring up and establish system resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, as with the term "network management," the term "systems management" is also used to refer to a myriad of other management functions and activities, of greater or lesser scope, which may also be applied to the management of resources other than system resources.

End of Document